


# Handbuch für den Administrator

Version 1026

WWW.REDDOXX.COM

# Copyright



**REDDOXX GmbH**
Saline 29

D-78628 Rottweil

Fon: +49 (0)741 248 810
Fax: +49 (0)741 248 811

E-Mail: info@reddoxx.com
Internet: http://www.reddoxx.com
Support: http://support.reddoxx.net

Revisionsnummer 3.2.5
Letzte Änderung: 29.09.2010

# Inhaltsverzeichnis

# 1 REDDOXX Handbuch

## 1.1 Symbolik und Hervorhebungen

Das Ihnen hier vorliegende Handbuch richtet sich an den Administrator der REDDOXX Appliance. Zur besseren Lesbarkeit des Handbuchs wird ausschließlich der "Administrator" angesprochen, gemeint ist damit sowohl die Administratorin als auch der Administrator.
Lesen Sie bitte das gesamte Handbuch genau durch, um den fachgerechten Einsatz der REDDOXX Appliance zu ermöglichen. Nur so können wir Ihnen die Bedienung der REDDOXX Appliance erleichtern.
Im Glossar finden Sie eine Zusammenstellung der verwendeten Fachausdrücke mit Erklärung.

**Die in diesem Handbuch verwendete Typografie bedeutet für Sie Folgendes:**

**GEFAHR / WARNUNG**

**Alle Warn- und Sicherheitshinweise in diesem Handbuch sind auf diese Weise gekennzeichnet. Halten Sie sich immer an die Vorschriften, damit keine Personen und/oder Gegenstände zu Schaden kommen.**

**HINWEIS**

Ein Hinweis oder Tipp macht auf besonders wichtige und hilfreiche Informationen zur REDDOXX Appliance aufmerksam. Nur wenn die REDDOXX Appliance gemäß den Empfehlungen des Herstellers transportiert, aufbewahrt, aufgestellt, installiert, bedient, betrieben und unterhalten wird, kann das Gerät richtig und fehlerfrei funktionieren.

| HERVORHEBUNG | BEISPIEL |
|---|---|
| Reiter | "Name des Reiters" |
| Feldbenennungen | *Benennung des Feldes* |
| Schaltflächen | SCHALTFLÄCHE |
| Auswahlliste | **Listeneintrag** |
| Listeneintrag in der Listenansicht | 'Eintrag' |

ı **Siehe auch:** Hier steht ein Verweis auf ein Kapitel.

**Benennungen**
Erklärung der jeweiligen Benennung.

## 1.2 Allgemeine Warn- und Sicherheitshinweise

Dieses Handbuch enthält Warn- und Sicherheitshinweise, welche Ihrem eigenen Schutz aber auch dem Schutz der REDDOXX Appliance dienen. Um Ihre Sicherheit nicht zu gefährden, beachten Sie unbedingt die folgenden Grundregeln für die Installation, die Benutzung und Bedienung der REDDOXX Appliance.

**Die Hinweise in diesem Handbuch sind wie folgt hervorgehoben:**

**GEFAHR**

**Das Unterlassen von Vorkehrungen und Sicherheitsmaßnahmen kann zu schwerwiegenden gesundheitlichen Schäden oder zu Verletzungen von Personen oder gar zu Todesfällen führen.**

**WARNUNG**

**Nur Fachpersonal ist es erlaubt, die Appliance zu bedienen oder mögliche Fehler in der Hardware zu beheben. Fachpersonal sind qualifizierte Personen, welche zur Inbetriebsetzung, Unterhalt, Steuerungsprogrammierung, Hardwarebedienung gemäß Sicherheitsvorschriften nach den gültigen Normen befugt sind und über eine entsprechende Ausbildung verfügen.**

**HINWEIS**

Beachten Sie die Einstellungen, die Sie in der REDDOXX Appliance vornehmen. Alle Einstellungen, die Sie vornehmen werden von der REDDOXX Appliance gespeichert, nicht von der REDDOXX Konsole. Die Konsole ist nur die Eingabemaske. Diese Hinweise finden Sie ausschließlich im Inhalt des Handbuchs.

**Lesen Sie sich die Warn- und Sicherheitshinweise vor Inbetriebnahme der REDDOXX Appliance gründlich durch:**

**GEFAHR/WARNUNG**

**Befolgen Sie alle auf der REDDOXX Appliance angebrachten und in diesem Handbuch aufgeführten Anweisungen.**

**Ziehen Sie vor der Reinigung der REDDOXX Appliance den Netzstecker. Verwenden Sie keine flüssigen oder aerosolhaltigen Reinigungsmittel. Benutzen Sie zur Reinigung nur ein feuchtes Tuch.**

**Verwenden Sie die REDDOXX Appliance nicht in der Nähe von Wasser. Verschütten Sie keine Flüssigkeit auf oder in die REDDOXX Appliance.**

**Stellen Sie die REDDOXX Appliance auf eine stabile Oberfläche.**

**Im Gehäuse befinden sich Öffnungen zur Belüftung. Diese Öffnungen dürfen nicht zugestellt oder verdeckt werden. Stellen Sie die REDDOXX Appliance nicht neben oder auf einem Heizkörper auf.**

**Verwenden Sie nur die am Netzanschluss angegebene Stromquelle. Sind Sie unsicher, welche Art von Stromquelle Sie haben, wenden Sie sich an Ihr örtliches Energieversorgungsunternehmen.**

**Laufen Sie nicht auf dem Kabel und stellen Sie nichts darauf.**

**Wenn Sie ein Verlängerungskabel für die REDDOXX Appliance verwenden, vergewissern Sie sich, dass die Gesamtstromstärke aller an dieses Verlängerungskabel angeschlossenen Geräte die zulässige Stromstärke für das Verlängerungskabel nicht überschreitet.**

**Stecken Sie keine Gegenstände in die Lüftungsschlitze der REDDOXX Appliance.**

**Versuchen Sie nicht, Ihre REDDOXX Appliance selbst zu warten, mit Ausnahme der in diesem Handbuch erklärten Fälle. Verändern Sie nur die in diesen Anweisungen erwähnten Steuerungen. Wenn Sie Abdeckungen öffnen, die mit "Warranty void if broken" versehen sind, könnten Sie sich hohen Stromspannungen oder anderen Risiken aussetzen. Überlassen Sie die Wartung dieser Teile dem Fachpersonal.**

**Tritt einer der folgenden Fälle ein, ziehen Sie den Netzstecker der REDDOXX Appliance aus der Steckdose und lassen Sie die REDDOXX Appliance von Fachpersonal warten:**

- **Die Leitung oder der Stecker sind beschädigt.**
- **Es wurde Flüssigkeit in die REDDOXX Appliance verschüttet.**
- **Die REDDOXX Appliance arbeitet trotz Befolgung der Anweisungen nicht ordnungsgemäß.**
- **Die REDDOXX Appliance wurde fallen gelassen, oder das Gehäuse ist beschädigt.**
- **Die REDDOXX Appliance weist erhebliche Leistungsänderungen auf.**

**Die REDDOXX Appliance immer vorsichtig transportieren. Durch Erschütterung oder Sturz kann auch das Innere des Geräts beschädigt werden. Beschädigte Geräte nicht in Betrieb nehmen!**

## 1.3 Allgemeiner Funktionsumfang

Vielen Dank für den Erwerb der REDDOXX Appliance und der dazugehörigen Konsole der Appliance. Die REDDOXX Appliance ist ein innovatives Produkt zur zuverlässigen, aktiven und individuellen Vermeidung und Abwehr von Spam-Problemen und zur gesetzeskonformen Archivierung von E-Mail. Des Weiteren können Sie geschäftkritische und sensible Informationen auch verschlüsselt zu Ihren Geschäftpartnern versenden, sodass Unbefugte selbst abgefangene E-Mails nicht einsehen können. Mit der REDDOXX Appliance schützen Sie Ihr Unternehmen vor technischen und wirtschaftlichen Schäden sowie vor Imageschäden.
Die REDDOXX Appliance filtert unerwünschte E-Mails und Spam von vornherein aus. Sie sparen viel Zeit, denn Viren, Würmer und Trojaner gelangen erst gar nicht in Ihr aktives Netzwerk. Die REDDOXX Appliance wird einfach vor den E-Mail-Server geschaltet und ist exakt auf die individuellen Bedürfnisse Ihres Unternehmens abgestimmt.

**Unsere Lösung ist ebenso ungewöhnlich wie erfolgreich:**
***Entgegen der herkömmlichen Vorgehensweise: "Herausfiltern, was nicht erwünscht ist" geht die REDDOXX Appliance den proaktiven Weg: "Vordefinieren, was Sie haben wollen".***

Die REDDOXX Appliance ist eine optimal aufeinander abgestimmte Einheit von Hardware und Software, die nur erwünschte E-Mails sofort selektiert und zustellt. Sie ist zwischen Firewall und E-Mail-Server installiert und erfordert somit nur minimalste Eingriffe in die IT Ihres Unternehmens.

**Die REDDOXX Appliance löst für Sie sofort vier vorrangige Probleme:**

1. Was für den einen Spam ist, ist für den anderen eine relevante Nachricht. Deshalb selektiert die REDDOXX Appliance die erwünschten Nachrichten und ermittelt in Zweifelsfällen die Relevanz der Nachricht durch Autorisierung des Versenders.
2. Durch die Vordefinition, weitere zusätzliche Filter und die interaktive Autorisierung des E-Mail-Versenders bietet die REDDOXX Appliance höchste Erfolgschancen bei der Bekämpfung von Spam und erzielt somit Ihre höchste Zufriedenheit.
3. Archivierung aller E-Mails durch MailDepot:
    1. Organisatorische Transparenz und Steigerung der Produktivität.
    2. Vermeidung von versehentlichem oder absichtlichem Löschen relevanter E-Mails.
    3. Zeitgewinn für Administratoren und User durch benutzerdefinierte. Zugriffsmöglichkeiten auf archivierte E-Mails.
4. Verschlüsselte E-Mail-Übertragung mit dem MailSealer

# 2 Die REDDOXX Appliance

**Informationen zu den REDDOXX Appliances**

Wir bieten Ihnen die maßgeschneiderte Lösung für Ihr Unternehmen. Dabei berücksichtigen wir Ihre individuellen Ansprüche, von der heutigen Zahl der Arbeitsplätze bis hin zur weiteren Entwicklung Ihres Unternehmens. Die verschiedenen Versionen stellen sicher, dass die REDDOXX Appliance allen Anforderungen kleiner, mittlerer wie auch großer Unternehmen gerecht wird.
Die REDDOXX Appliance ist modular aufgebaut: Sie besteht aus den Produkten

- REDDOXX Spamfinder
- REDDOXX MailDepot
- REDDOXX MailSealer

**Die REDDOXX Appliance ist in folgenden unterschiedlichen Hardware Varianten für Sie erhältlich:**

- RX-50
- RX-100
- RX-250
- RX-750
- RX-2500

**REDDOXX Allgemein:**

- Einfacher Aufbau für schnellen Einsatz innerhalb von Minuten und gleichzeitige Kompatibilität mit allen standardisierten E-Mail-Servern.
- Sicherer, gehärteter Linux-Kernel.
- Leistungsfähigen Virenschutz durch die Open Source Software ClamAV.

**REDDOXX Spamfinder:**

- Leistungsfähige Spam-Filterung inklusive CISS Technologie, welche eine bis zu 100%ige Spam-Reduktion liefert.
- Innovativer Advanced Realtime Blacklist Filter, Whitelist Filter sowie zusätzliche Statistikfilter und weitere Inhalts- und Blacklist Filter Technologien.
- Möglichkeit automatisierte und externe Backups zu erstellen.

**REDDOXX MailDepot:**

- Automatische revisions- und manipulationssichere Archivierung aller E-Mails
- Organisatorische Transparenz und Steigerung der Produktivität

Die REDDOXX Appliance ist zwischen Firewall und E-Mail-Server installiert und erfordert somit nur minimalste Eingriffe in die IT Ihres Unternehmens.

**REDDOXX MailSealer:**

- schnelle Verschlüsselung und Signatur von E-Mails
- kompatibel zu allen gängigen E-Mail-Programmen
- unterstützt S/MIME

**HINWEIS**

Bitte entnehmen Sie die Hardware Daten Ihrer REDDOXX Appliance dem Kapitel "REDDOXX Appliances - Technische Daten".

## 2.1 Die REDDOXX Appliance – RX-50

Die REDDOXX Appliance - RX-50 ist für die Anforderungen kleiner und mittelständischer Unternehmen bis ca. 50 User gedacht




Abbildung: REDDOXX Appliance - RX-50

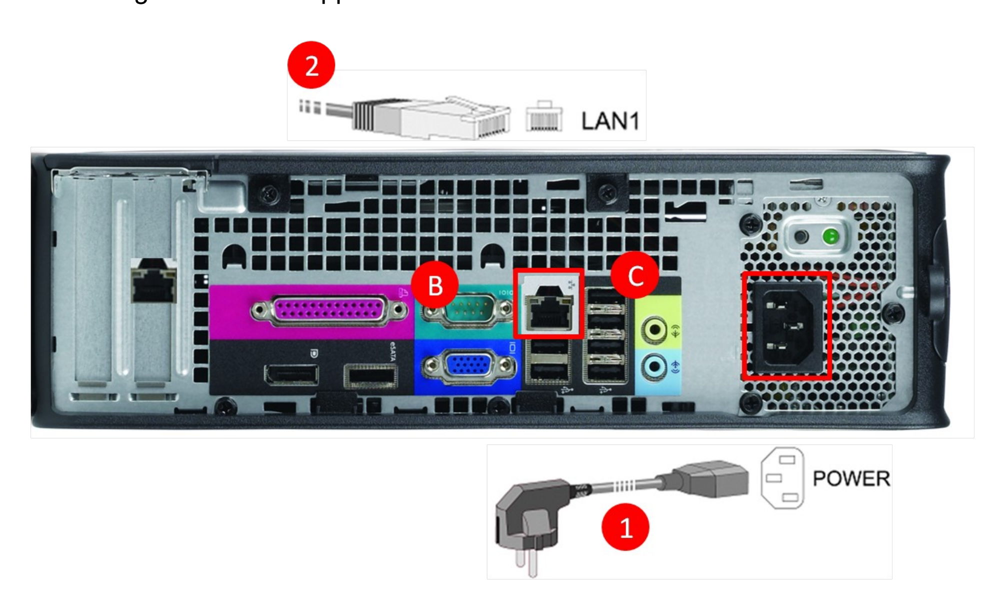



Abbildung: Anschlüsse der REDDOXX RX-50 Appliance

| BESTANDTEILE | SO SCHLIESSEN SIE DIE REDDOXX APPLIANCE RICHTIG AN |
|---|---|
| 1. REDDOXX Appliance | Verbinden Sie die REDDOXX Appliance mit dem Netzstecker (1). |
| 2. Netzstecker | Stecken Sie den Netzstecker (1) in eine geeignete Steckdose. |
| 3. Netzwerkkabel | Stecken Sie Ihr Netzwerkkabel in LAN-1(2) ein. |
| | |
| A Ein/Ausschalter | Schalten Sie die REDDOXX Appliance an. (Vorderseite) |
| B Bildschirmanschluss | Nur für Wartungszwecke. |
| C USB | Nur für Wartungszwecke (Tastatur). |

**ACHTUNG**

**Beachten Sie unbedingt die angegebenen Warn- und Sicherheitshinweise und alle weiteren relevanten Informationen zum fachgerechten Umgang mit der REDDOXX Appliance.**

## 2.2 Die REDDOXX Appliance – RX-100

Die REDDOXX Appliance - RX-100 ist für die Anforderungen mittelständischer Unternehmen bis ca. 100 User gedacht.




Abbildung: REDDOXX Appliance - RX-100 mit Frontabdeckung




Abbildung: REDDOXX Appliance - RX-100 ohne Frontabdeckung

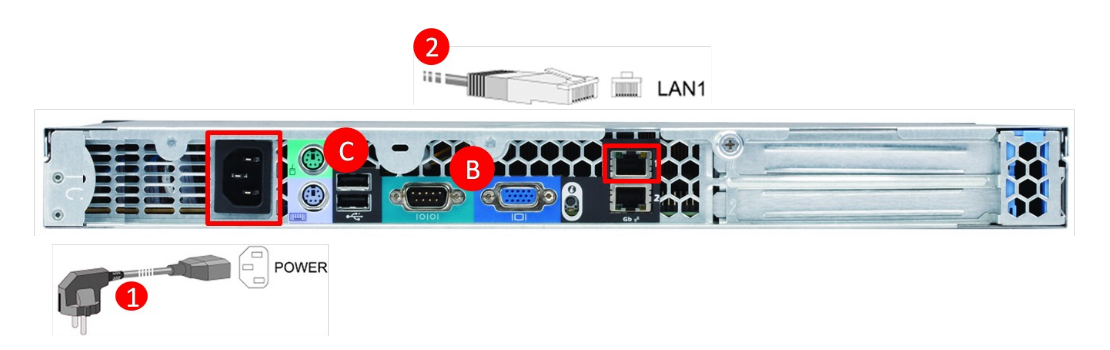



Abbildung: Anschlüsse der REDDOXX RX-100 Appliance

| Bestandteile | So schliessen Sie die REDDOXX Appliance richtig an |
|---|---|
| 1. REDDOXX Appliance | Verbinden Sie die REDDOXX Appliance mit dem Netzstecker (1). |
| 2. Netzstecker | Stecken Sie den Netzstecker (1) in eine geeignete Steckdose. |
| 3. Netzwerkkabel | Stecken Sie Ihr Netzwerkkabel in LAN-1(2) ein. |
| | |
| A Ein/Ausschalter | Schalten Sie die REDDOXX Appliance an. (Vorderseite) |
| B Bildschirmanschluss | Nur für Wartungszwecke. |
| C USB | Nur für Wartungszwecke (Tastatur). |

**Achtung**

**Beachten Sie unbedingt die angegebenen Warn- und Sicherheitshinweise und alle weiteren relevanten Informationen zum fachgerechten Umgang mit der REDDOXX Appliance**

## 2.3 Die REDDOXX Appliance – RX-250

Die REDDOXX Appliance - RX-250 ist für die Anforderungen größerer Unternehmen bis ca. 250 User gedacht.




Abbildung: REDDOXX Appliance - RX-250 mit Frontabdeckung




Abbildung: REDDOXX Appliance - RX-250 ohne Frontabdeckung

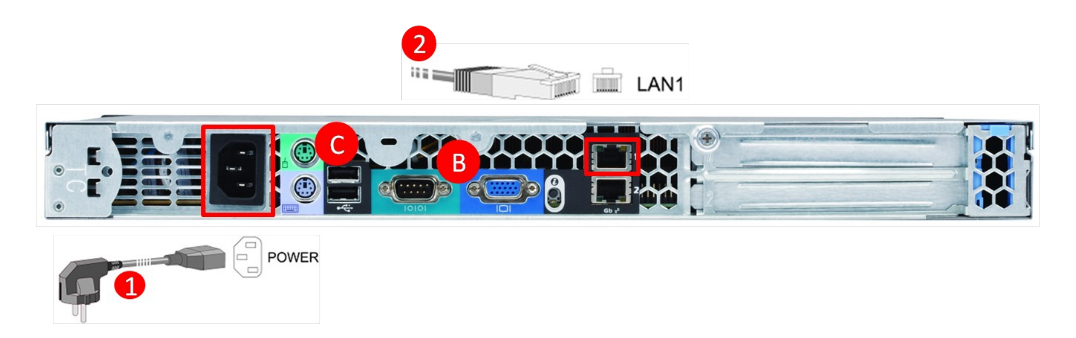



Abbildung: Anschlüsse der REDDOXX RX-250 Appliance

| BESTANDTEILE | SO SCHLIESSEN SIE DIE REDDOXX APPLIANCE RICHTIG AN |
|---|---|
| 1. REDDOXX Appliance | Verbinden Sie die REDDOXX Appliance mit dem Netzstecker (1). |
| 2. Netzstecker | Stecken Sie den Netzstecker (1) in eine geeignete Steckdose. |
| 3. Netzwerkkabel | Stecken Sie Ihr Netzwerkkabel in LAN-1(2) ein. |
| | |
| A Ein/Ausschalter | Schalten Sie die REDDOXX Appliance an. (Vorderseite) |
| B Bildschirmanschluss | Nur für Wartungszwecke. |
| C USB | Nur für Wartungszwecke (Tastatur). |

**ACHTUNG**

**Beachten Sie unbedingt die angegebenen Warn- und Sicherheitshinweise und alle weiteren relevanten Informationen zum fachgerechten Umgang mit der REDDOXX Appliance**

## 2.4 Die REDDOXX Appliance – RX-750

Die REDDOXX Appliance - RX-750 ist für die Anforderungen von großen Unternehmen bis ca. 750 User gedacht.




Abbildung: REDDOXX Appliance - RX-750 mit Frontabdeckung




Abbildung: REDDOXX Appliance - RX-750 ohne Frontabdeckung

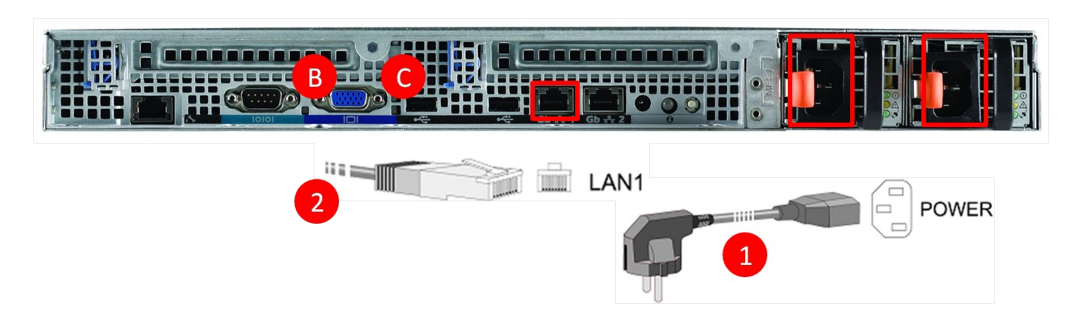



Abbildung: Anschlüsse der REDDOXX RX-750 Appliance

| Bestandteile | So schliessen Sie die REDDOXX Appliance richtig an |
|---|---|
| 1. REDDOXX Appliance | Verbinden Sie die REDDOXX Appliance mit dem Netzstecker (1). |
| 2. Netzstecker | Stecken Sie den Netzstecker (1) in eine geeignete Steckdose. |
| 3. Netzwerkkabel | Stecken Sie Ihr Netzwerkkabel in LAN-1(2) ein. |
| | |
| A Ein/Ausschalter | Schalten Sie die REDDOXX Appliance an. (Vorderseite) |
| B Bildschirmanschluss | Nur für Wartungszwecke. |
| C USB | Nur für Wartungszwecke (Tastatur). |

**Achtung**

**Beachten Sie unbedingt die angegebenen Warn- und Sicherheitshinweise und alle weiteren relevanten Informationen zum fachgerechten Umgang mit der REDDOXX Appliance**

## 2.5 Die REDDOXX Appliance – RX-2500

Die REDDOXX Appliance - RX-2500 ist für die Anforderungen von sehr großen Unternehmen bis ca. 2500 User gedacht.

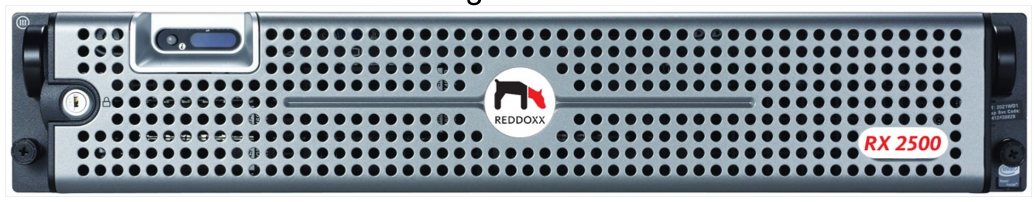



Abbildung: REDDOXX Appliance - RX-2500 mit Frontabdeckung




Abbildung: REDDOXX Appliance - RX-2500 ohne Frontabdeckung

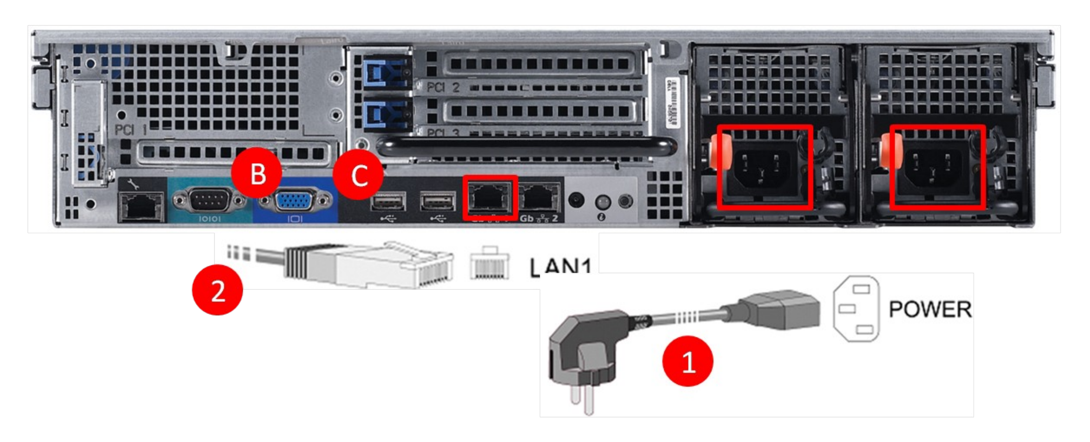



Abbildung: Anschlüsse der REDDOXX RX-2500 Appliance

| Bestandteile | So schliessen Sie die REDDOXX Appliance richtig an |
|---|---|
| 1. REDDOXX Appliance | Verbinden Sie die REDDOXX Appliance mit dem Netzstecker (1). |
| 2. Netzstecker | Stecken Sie den Netzstecker (1) in eine geeignete Steckdose. |
| 3. Netzwerkkabel | Stecken Sie Ihr Netzwerkkabel in LAN-1(2) ein. |
| | |
| A Ein/Ausschalter | Schalten Sie die REDDOXX Appliance an. (Vorderseite) |
| B Bildschirmanschluss | Nur für Wartungszwecke. |
| C USB | Nur für Wartungszwecke (Tastatur). |

**Achtung**

**Beachten Sie unbedingt die angegebenen Warn- und Sicherheitshinweise und alle weiteren relevanten Informationen zum fachgerechten Umgang mit der REDDOXX Appliance**

## 2.6 Technische Daten

| Hardware Appliance | RX-50 | RX-100 | RX-250 | RX-750 | RX-2500 |
|---|---|---|---|---|---|
| Basis | DELL OP 760 | DELL CR100 | DELL R200 | DELL R300 | DELL PE 2950 |
| Queuekapazität | 60 GB | 100 GB | 120 GB | 280 GB | 1000 GB |
| Empfohlene Anzahl User | 50 | 100 | 250 | 750 | 2500 |
| Raid-Level | n.a. | n.a. | RAID 1 | RAID 1 | RAID 5, Hotplug |
| Prozessor | 1x Intel Cel 440 2,0 GHz | 1x Intel Cel 440 2,0 GHz | 1X Intel DC E2200 | 1X Intel DC E6305 | 2x Intel QC E5420 |
| Speicher (RAM) | 512 MB | 512 MB | 1 GB | 2 GB | 4 GB |
| Ausführung | Desktop . | 19" Short Rack 1U | 19" Rackmount 1U | 19" Rackmount 1U | 19" Rackmount 2U |
| Maße (B x H x T) | 31.4 x 9.26 x 34 cm | 44,7 x 4,27 x 45,61 cm | 44,7 x 4,27 x 54,61 cm | 42,63 x 4,24 x 66,04 cm | 44,3 x 8,64 x 74,4 cm |
| Gewicht | 7 kg | 8,9 KG | 11,8 Kg | 13,5 Kg | 23 Kg |
| Spannung | 100-240 V | 100-240 V | 100-240 V | 100-240 V | 100-240 V |
| Eingangsstrom / Frequenz | 5-3A / 50-60 Hz | 5-3A / 50-60 Hz | 5-3A / 50-60 Hz | 5-3A / 50-60 Hz | 5-3A / 50-60 Hz |
| Betriebsstemperatur | 10° -40° | 10° -35° | 10° -35° | 10° -35° | 10° -35° |
| Relative Luftfeuchtigkeit | 8-90% non-condensing | 8-90% non-condensing | 8-90% non-condensing | 20-90% non-condensing | 20-90% non-condensing |
| Zertifizierung | CE | CE | CE | CE | CE |

| Virtual Appliance | RX-50 | RX-100 | RX-250 | RX-750 | RX-2500 |
|---|---|---|---|---|---|
| Empfohlene Anzahl User | 50 | 100 | 250 | 750 | 2500 |
| benötigter Speicher (RAM) | 256 MB | 512 MB | 1024 MB | 2 GB | 4 GB |
| Anzahl Prozessoren | 1 | 1 | 1 | 1 | 1 |

## 2.7 Lieferumfang

Bitte überprüfen Sie vor dem Installieren Ihre Lieferung auf Vollständigkeit. Im Lieferumfang sind folgende Produkte enthalten:

- REDDOXX Appliance
- Software für die REDDOXX Konsolen auf CD
- Administrator-Konsole
- Benutzer-Konsole
- "Handbuch für den Administrator" und "Handbuch für den Benutzer" als PDF

**HINWEIS**

Die aktuellste Version der REDDOXX Software und Handbücher finden Sie im Support-Bereich unter http://support.reddoxx.net

# Übernahme

Überprüfen Sie bei der Übernahme das Produkt auf Beschädigungen.
Sollten Sie bei der Anlieferung oder beim Auspacken der Ware einen offensichtlichen Schaden feststellen, so sollten wenden Sie sich an Ihren Fachhändler.

**WARNUNG**

**Gerät immer vorsichtig transportieren. Durch Erschütterung oder Sturz kann auch das Innere des Geräts beschädigt werden. Beschädigte Geräte nicht in Betrieb nehmen!**

# 3 Die ersten Schritte

## 3.1 Allgemeine Informationen

Dieses Kapitel soll Ihnen die erste Inbetriebnahme der REDDOXX Appliance erleichtern und fasst alle notwendigen Schritte zusammen, um die REDDOXX Appliance einsatzbereit zu machen. Zuerst aber zeigen wir Ihnen schematisch, an welcher Stelle Sie die REDDOXX Appliance installieren müssen. Die weiteren Kapitel beschäftigen sich mit dem Anschluss, der Anmeldung, der Grundkonfiguration und der Bedienung Ihrer REDDOXX Appliance.

### 3.1.1 Funktionsbeschreibung

Die REDDOXX Appliance verhält sich gegenüber dem Absender wie ein E-Mail-Server. Schon während sich die Verbindung zwischen dem sendenden E-Mail-Server und der REDDOXX Appliance aufbaut, werden die ersten Filter aktiv. Je nach Filtereinstellung kann es bereits in dieser Phase zu einer Ablehnung der E-Mail durch die REDDOXX Appliance kommen.

ı **Siehe auch:** "Filter"

Die REDDOXX Appliance kann mehrere E-Mail-Domänen verwalten und auf unterschiedliche E-Mail-Server in Ihrem Unternehmen die jeweiligen E-Mails abgeben.

### 3.1.2 Integration und Inbetriebnahme

Die standardmäßige Einrichtung besteht aus einem oder mehreren E-Mail-Servern und der Appliance, welche zwischen dem E-Mail-Server und Ihrer Firewall eingebunden werden.

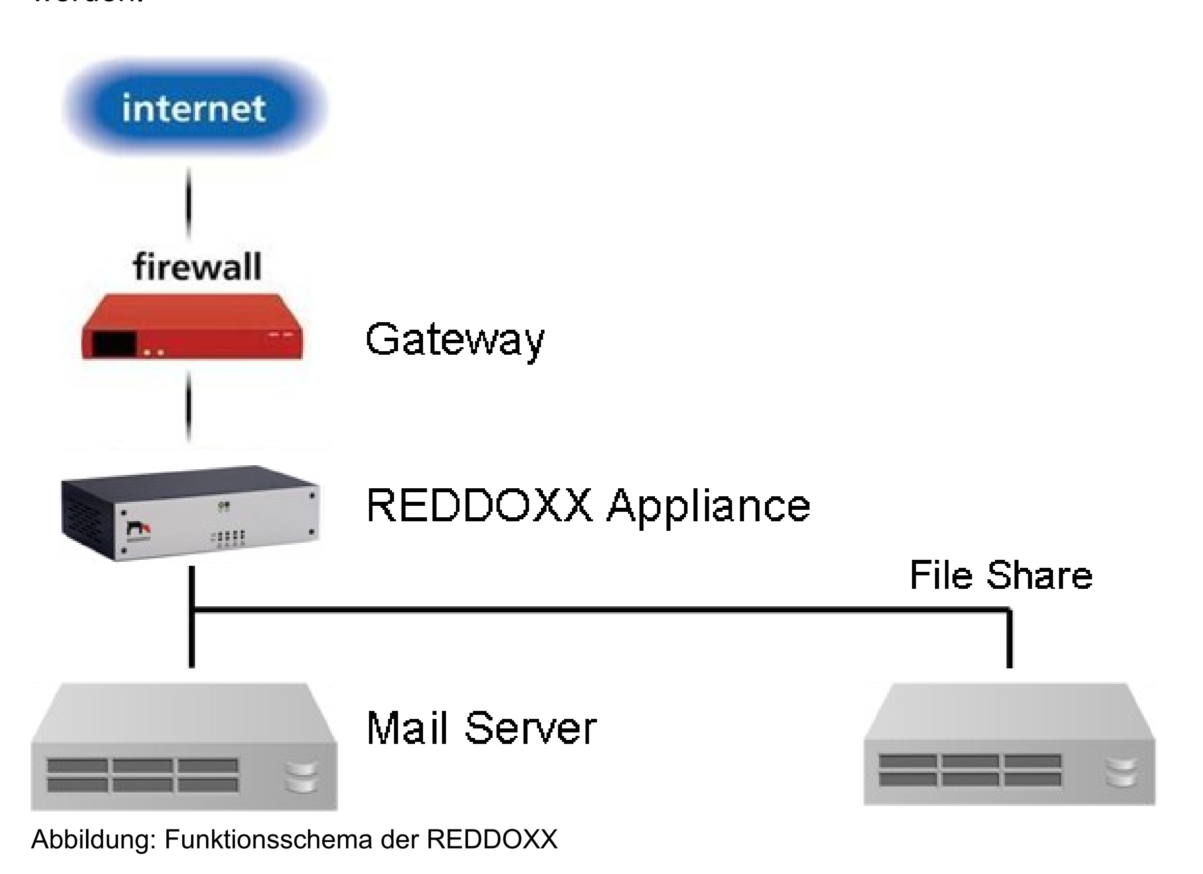



Abbildung: Funktionsschema der REDDOXX

Zur Inbetriebnahme der REDDOXX, sind nur wenige Handgriffe notwendig:

- Die REDDOXX Appliance mit dem Netzwerk verbinden,
- eine IP-Adresse zuweisen und
- Sie müssen das Routing des E-Mail-Verkehrs so anpassen, dass eingehende E-Mails möglichst früh auf die REDDOXX Appliance geleitet werden, damit die REDDOXX Appliance die weitere Zustellung übernehmen kann.

Nähere Informationen finden Sie in der folgenden Kurzanleitung.

**TIPP**

Für die effiziente Bekämpfung von Spam empfehlen wir, dass die REDDOXX Appliance unmittelbar hinter Ihrer Firewall als so genannten ersten "Mailhop" installiert wird. Dies bewirkt, dass der Absender die Verbindung direkt mit der REDDOXX Appliance aufbaut.

Da die REDDOXX Appliance in der Lage ist aus ihren Aktionen zu lernen, empfehlen wir, dass Sie auch den ausgehenden E-Mail-Verkehr durch die REDDOXX Appliance leiten.

### 3.1.3 Firewall - Portliste

Diese Ports müssen für einen einwandfreien Betrieb der REDDOXX Appliance geöffnet werden:

**SMTP/25 TCP in/out**
Für ein- und ausgehende E-Mails

**DNS/53 UDP/TCP out**
Für Domain Name Service Anfragen an Ihren DNS-Server.

**HTTP/80 TCP out**
Für die Kommunikation mit dem REDDOXX-Portal. Dort werden die Lizenzinformationen überprüft.
Für den REMOTE SUPPORT SERVICE . Bei technischen Problemen kann der REDDOXX Support Mitarbeiter sich auf die Appliance schalten, sofern zuvor vom Administrator der Service gestartet wurde.
Für Software und Pattern-Updates, sowie Spam-Validierungen.

**NTP/123 UDP out**
Für den Zeitabgleich mit einem Zeit-Server

**SMB 137,138 UDP out, 139 TCP out, CIFS 445 TCP out**
für das Backup und die Archivierung (Maildepot) auf einen Remote Windows/Samba-Share.

**LDAP/389 TCP out, LDAP/636 out für SSL**
für die Benutzerautentifizierung und Empfängerüberprüfung via Active Directory, OpenLDAP, Novell eDircetory, Lotus Notes Domino.

**LDAP/3268 TCP out**
Für schnelle LDAP-Abfragen gegen einen Global Catalog Server.

**REDDOXX/4010 TCP in**
Für die User- und Administratorkonsole der REDDOXX-Appliance.
**REDDOXX/4011 TCP in**
Für die Kommunikation zw. Administratorkonsole und dem Control Service Port der Appliance, erforderlich für den Cluster Manager, die Diagnose und den Remote Support Service.
**REDDOXX/55555 TCP out**
Für die Kommunikation mit dem Fuzzy-Filter Remote Service zur Spamerkennung.

**HINWEIS**

Achten Sie auf die erwähnten Ports insbesondere, wenn die REDDOXX in einem anderen Netzwerksegement, wie z.B. einer DMZ steht, und vom internen LAN durch eine Firewall getrennt ist.

## 3.2 Kurzanleitung zur Grundkonfiguration

### 3.2.1 Der Anschluss und die Netzwerkkonfiguration

**REDDOXX Appliance anschließen**

Um die REDDOXX Appliance in Ihr System einbinden zu können, gehen Sie wie folgt vor.

**Voraussetzungen:** Lesen der Warn- und Sicherheitshinweise.

1. Schließen Sie die REDDOXX Appliance an die **Stromversorgung** an.
2. Schließen Sie einen **Monitor** und eine **Tastatur** an.
3. **Schalten** Sie die REDDOXX Appliance **ein**.
   Die IP-Adresse lautet *192.168.0.1*.
4. Melden Sie sich als Benutzer „***admin***“ mit dem Passwort „***AppAdmin***“ an. Es erscheint das **Administrations-Menü**. Weitere Details und Screenshots finden Sie im Kapitel 6. - Appliance Konsole.
5. Wählen Sie den Punkt – ***Settings***
6. Wählen Sie den Punkt – ***Network***
7. Geben Sie die ***Netzwerk-Kenndaten*** ein. (*Hostname, Domain, IP-Address, Netmask, Gateway, 1. DNS, 2. DNS*)
8. Drücken Sie die TAB-Taste um auf ***OK*** zu gelangen und drücken Sie die ENTER-Taste. Das Netzwerkinterface wird nun neu initialisiert.
9. Wählen Sie ***BACK*** aus, um ins Hauptmenü zu gelangen.
10. Wählen Sie ***EXIT*** aus, um das Konsolenprogramm zu beenden.
11. Schließen Sie ein ***Netzwerkkabel*** (RJ45) an und verbinden Sie die Appliance mit Ihrem Netzwerk.
12. Fahren Sie die Konfiguration mit der ***Admin-Konsole*** fort, die im nachfolgenden Kapitel beschrieben ist.

**HINWEIS**

Funktionsbeschreibung und genaue Anschlüsse der REDDOXX Appliance finden Sie im Haupt-Kapitel bei den verschiedenen Modell-Varianten.

### 3.2.2 Die Anmeldung

**Anmeldung ausführen**

Die REDDOXX Appliance ist aus Sicherheitsgründen ausschließlich über die Anmeldung zugänglich. Daher ist es notwendig, dass Sie sich wie folgt mit Benutzername und Kennwort authentifizieren.

**Voraussetzungen:** Erwerb der REDDOXX Appliance mit den gültigen Lizenzen.

1. Kopieren Sie den Inhalt der REDDOXX CD auf Ihren Rechner.
   Die Dateien können in ein beliebiges Verzeichnis kopiert werden.
2. Klicken Sie doppelt auf die Datei *rdxadmin.exe.*
   Das Anmeldefenster öffnet sich.




Abbildung: Anmeldefenster

2. *Hostname:* Geben Sie den Hostnamen ein, zu dem Sie sich verbinden möchten oder wählen Sie ihn aus der Liste aus. Die Liste enthält die bisherigen Eingaben, die Sie bereits vorgenommen haben.
3. *Benutzername:* Geben Sie *sf-admin* ein.
4. Geben Sie das *Kennwort* ein.

**HINWEIS**

Folgende Standardwerte sind bei der Auslieferung der REDDOXX Appliance eingestellt: *Benutzername:* sf-admin und *Kennwort:* admin

6. Wählen Sie bei Realm die Option „local“ aus.
7. Wählen Sie die gewünschte *Sprache* in der Auswahlliste aus, in der Ihr Programm angezeigt werden soll.
   Die Auswahl beinhaltet die derzeit installierten Sprachen.
   Klicken Sie auf die Schaltfläche OK.

   Das Willkommenfenster öffnet sich.



Abbildung: Willkommenfenster

7. Klicken Sie auf die Schaltfläche SETUP-ASSISTENT um den Assistenten für die erste Konfiguration der REDDOXX Appliance zu starten.

**HINWEIS**

Führen Sie den Setup-Assistenten nur einmalig aus.

### 3.2.3 Die Grundkonfiguration

**Netzwerkeinstellungen vornehmen**

Der Setup Assistent führt Sie zur Erleichterung der Grundkonfiguration durch alle relevanten Einstellungen.

**Voraussetzungen:** Fenster für die Netzwerkeinstellungen ist aktiv.

**HINWEIS**

Wurden die Netzwerkeinstellungen der Appliance zuvor über die Appliance-Konsole konfiguriert (Kapitel 3.2.1) so können Sie hier die Kenndaten einfach übernehmen.

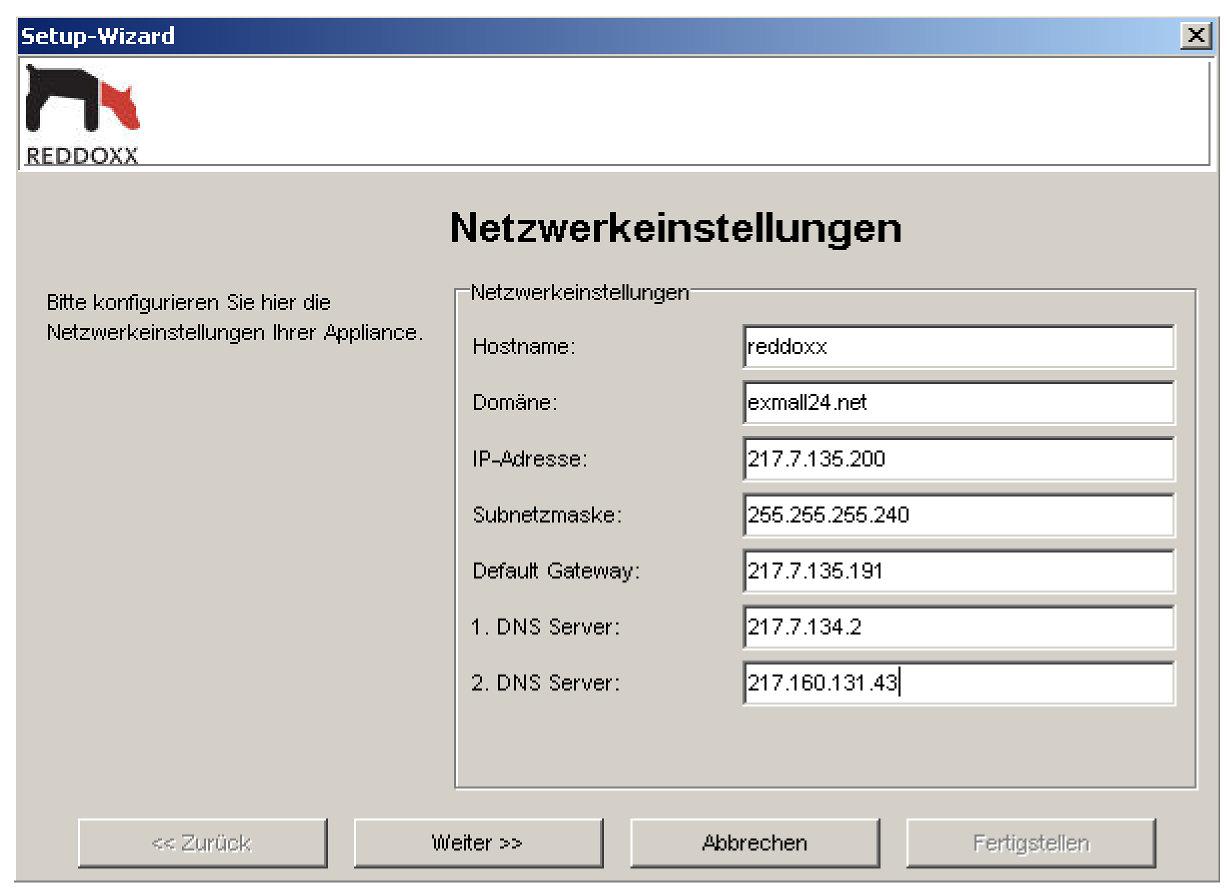



Abbildung: Grundkonfiguration - Netzwerkeinstellungen

1. Geben Sie einen *Hostname* ein.
2. Geben Sie eine/Ihre *Domäne* ein.
3. Geben Sie die *IP-Adresse* der REDDOXX Appliance an.

4. Geben Sie die entsprechende *Subnetzmaske* an.
5. Geben Sie die *Standard-Gateway* für die Internetanbindung an.
6. Geben Sie mindestens einen *DNS-Server* an.

**HINWEIS**

Achten Sie darauf, dass der DNS Server erreichbar ist, insbesondere, wenn die REDDOXX Appliance in einer DMZ steht.

7. Klicken Sie zum Fortfahren der Grundkonfiguration auf die Schaltfläche WEITER.
   ABBRECHEN: Änderungen verwerfen und Schließen der Grundkonfiguration.

**E-Mail-Domänen hinzufügen**

Über die E-Mail-Domänen sind Sie in der Lage, alle Domänen hinzuzufügen, für die die REDDOXX Appliance E-Mails empfangen soll.
**Voraussetzungen:** Fenster für die E-Mail-Domänen ist aktiv.

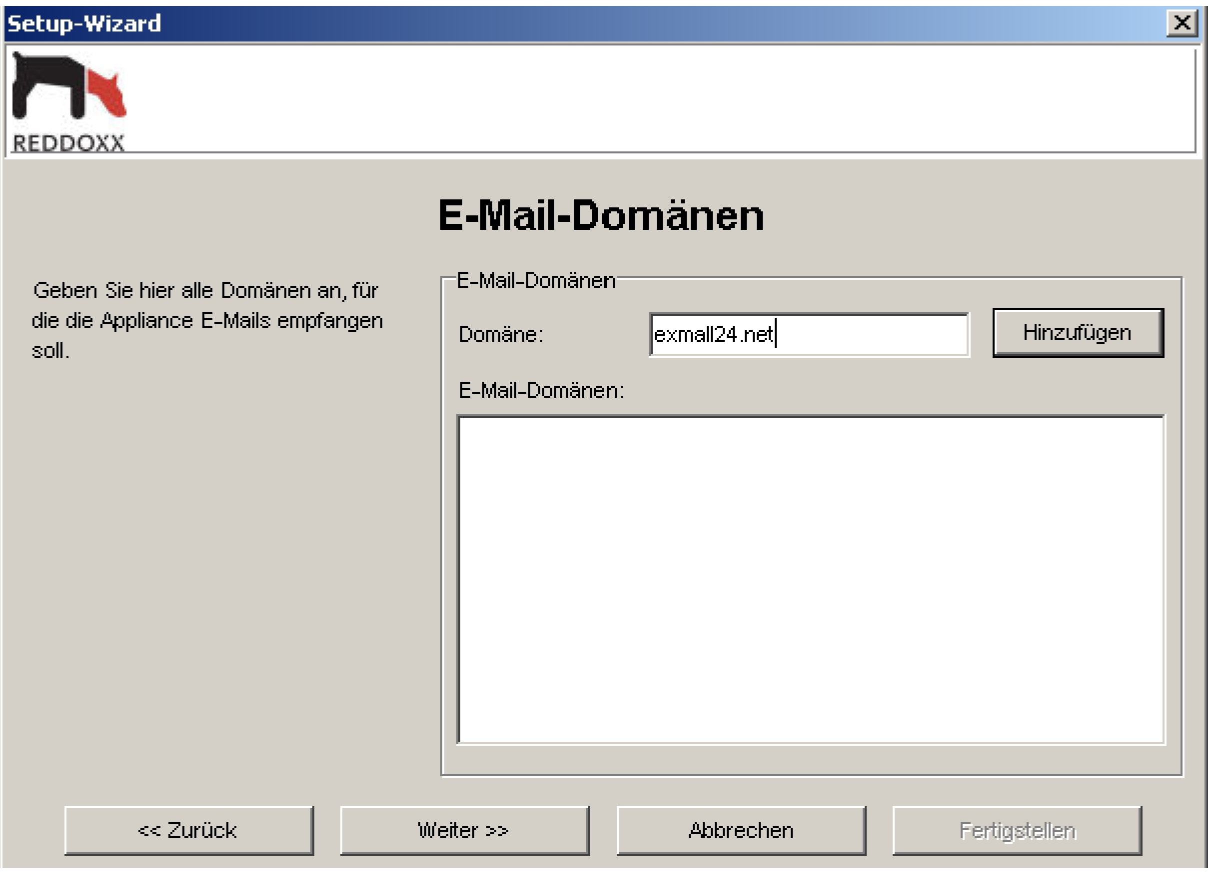



Abbildung: Grundkonfiguration - E-Mail-Domänen

1. Geben Sie alle Domänen an, für die Sie E-Mails empfangen möchten.
2. Klicken Sie auf die Schaltfläche HINZUFÜGEN.
   Die eingegebenen E-Mail-Domänen werden im Feld E-Mail-Domänen gelistet.

**HINWEIS**

Bitte achten Sie auf die richtige Schreibweise der E-Mail-Domänen. Für andere Domänen kann die REDDOXX Appliance keine E-Mails empfangen.

3. Klicken Sie zum Fortfahren der Grundkonfiguration auf die Schaltfläche WEITER.
   ZURÜCK: Wechseln zum vorherigen Fenster.
   ABBRECHEN: Änderungen verwerfen und Schließen der Grundkonfiguration.

**HINWEIS**

Um eine hinzugefügte Domäne wieder zu löschen, markieren Sie den entsprechenden Eintrag mit einem Mausklick und löschen Sie ihn mit der Entf-Taste auf Ihrer Tastatur. Dieser Vorgang kann nicht rückgängig gemacht werden.

**Lokale Netzwerke hinzufügen**

Über die Lokalen Netzwerke können Sie alle lokalen Netzwerke hinzufügen, für die die REDDOXX Appliance als E-Mail-Relay funktionieren soll. Somit kann die REDDOXX Appliance nicht als offenes E-Mail-Relay missbraucht werden, wenn E-Mails über die REDDOXX Appliance von Innen nach Außen geschickt werden.

**Voraussetzungen:** Fenster für Lokale Netzwerke ist aktiv.




Abbildung: Grundkonfiguration - Lokale Netzwerke

1. Geben Sie das *IP-Netzwerk* an, welches Mails an die REDDOXX Appliance senden darf.
2. Geben Sie die *Subnetzmaske* an. Mit der Subnetmaske 255.255.255.255 wird ein einzelner Host (z.B.192.168.0.8) hinzugefügt.

**HINWEIS**

Anstelle eines ganzen Netzes können Sie auch einzelne IP-Adressen, wie z.B. die Ihres Mailservers angeben. Einzelne IP-Adressen müssen mit 255.255.255.255 maskiert werden.

3. Klicken Sie auf die Schaltfläche HINZUFÜGEN.
   Die eingegebenen Lokalen Netzwerke werden im Feld Lokale Netze gelistet.

Sollten Sie mehrere E-Mail-Server in unterschiedlichen IP-Netzwerken haben, fügen Sie bitte auch diese Netze bzw. Hosts hinzu.

4. Klicken Sie zum Fortfahren der Grundkonfiguration auf die Schaltfläche WEITER.
   ZURÜCK: Wechseln zum vorherigen Fenster.
   ABBRECHEN: Änderungen verwerfen und Schließen der Grundkonfiguration.

**HINWEIS**

Um ein hinzugefügtes Netzwerk wieder zu löschen, markieren Sie den entsprechenden Eintrag mit einem Mausklick und löschen Sie ihn mit der Entf-Taste auf Ihrer Tastatur. Dieser Vorgang kann nicht rückgängig gemacht werden.

### E-Mail-Zustellung Konfigurieren

Über die E-Mail-Zustellung können Sie angeben, wohin die REDDOXX Appliance die E-Mails weiterleiten soll.

**Voraussetzungen:** Fenster für E-Mail-Zustellung ist aktiv.

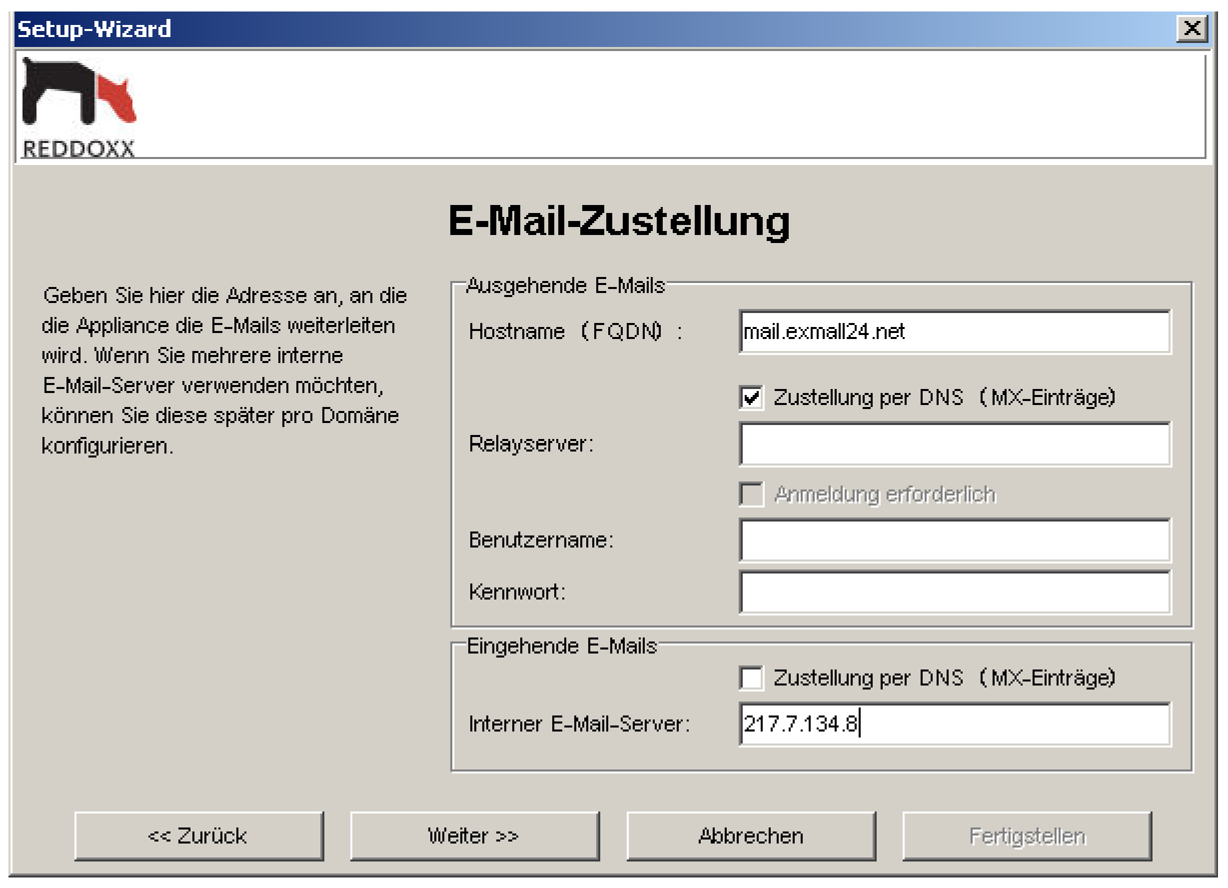



Abbildung: Grundkonfiguration - E-Mail-Zustellung

1. *Ausgehende E-Mails:*
   Tragen Sie den FQDN (hostname) ein.
   Aktivieren Sie gegebenenfalls die Option *Zustellung per DNS*, wenn die Zustellung der E-Mails über DNS erfolgen soll.

**HINWEIS**

Geben Sie den Hostname im FQDN-Format (Fully Qualified Domain Name) ein. Es wird dringend empfohlen, einen Hostnamen zu verwenden, der über eine Reverse-DNS Abfrage (PTR-Eintrag) auflösbar ist, sofern ausgehende Mails NICHT über einen Smarthost (Relay) geleitet werden.

2. Geben Sie den *Relay-Server* an, wenn Ihre ausgehenden E-Mails über ein Relay versendet werden müssen.
3. Aktivieren Sie die Option *Anmeldung erforderlich*, wenn der Relay-Server eine Authentifizierung erfordert.
4. Geben Sie *Benutzername* und *Passwort* ein, falls Sie bei Schritt 3 die Option aktiviert haben.
5. *Eingehende E-Mails:*
   Aktivieren Sie gegebenenfalls die Option *Zustellung per DNS*, wenn die Zustellung der E-Mails über DNS erfolgen soll.
6. Geben Sie bei *Interner E-Mail-Server* einen internen E-Mail-Server an.

   **HINWEIS**

   Falls Sie mehrere interne E-Mail-Server haben, können Sie diese später pro Domäne konfigurieren.

7. Klicken Sie zum Fortfahren der Grundkonfiguration auf die Schaltfläche WEITER.
   ZURÜCK: Wechseln zum vorherigen Fenster.
   ABBRECHEN: Änderungen verwerfen und Schließen der Grundkonfiguration.

**E-Mail-Adressen festlegen**

Hier wird die E-Mail-Adresse des Administrators und der REDDOXX Appliance verwaltet, die die REDDOXX Appliance zur Übermittlung von Systemmeldungen benötigt. Die E-Mail-Adresse des Administrators wird von der REDDOXX Appliance zur Kommunikation mit dem Administrator genutzt. Die E-Mail-Adresse der REDDOXX Appliance wird zur Kommunikation mit dem REDDOXX Portal genutzt.

**Voraussetzungen:** Fenster für E-Mail-Adressen ist aktiv.

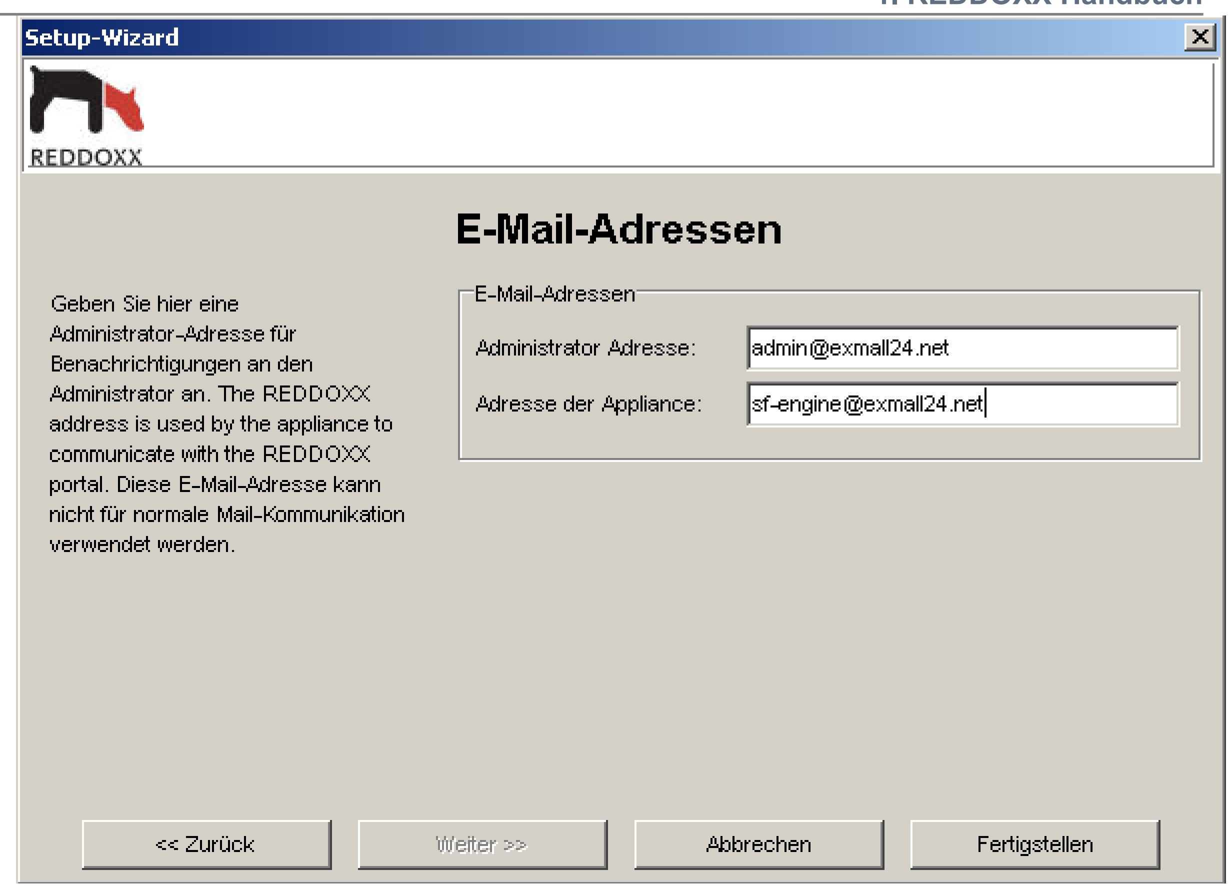


Abbildung: Grundkonfiguration - E-Mail-Adressen

1. Geben Sie im Feld *Administrator-Adresse* die E-Mail-Adresse des Administrators ein.
   Die *Administrator-Adresse* muss auf einem Ihrer E-Mail-Server existieren. Unter dieser Adresse erhalten Sie Mitteilungen bezüglich Neuerungen (Release Notes) und Updates der REDDOXX Appliance.
2. Geben Sie im Feld *REDDOXX-Adresse* die E-Mail-Adresse der REDDOXX Appliance ein.

**HINWEIS**

Die E-Mail-Adresse der REDDOXX Appliance ist für den systeminternen Betrieb erforderlich und darf nicht anderweitig verwendet werden.
Achten Sie darauf, die diese E-Mail-Adresse nicht auf Ihrem Mailserver existiert und dass sie von evt. vorgeschalteten Firewalls oder Relays weitergeleitet wird.

3. Klicken Sie zum Abschließen der Grundkonfiguration auf die Schaltfläche FERTIGSTELLEN.
   ZURÜCK: Wechseln zum vorherigen Fenster.
   ABBRECHEN: Änderungen verwerfen und Schließen der Grundkonfiguration.

# 4 Die Administrator Konsole

### Informationen zur Administrator-Konsole

Dieses Kapitel erklärt Ihnen den genauen Umgang mit der Administrator Konsole. Die Administrator-Konsole wurde konzipiert, um die Handhabung der REDDOXX Appliance zu erleichtern. Über die Konsole können Sie zu jeder Zeit alle Einstellungen der REDDOXX Appliance ergänzen oder ändern. Bevor Sie zum eigentlichen Anwendungsfenster der REDDOXX Appliance Konsole gelangen, müssen Sie sich anmelden.

### Anmeldung ausführen

Die REDDOXX Appliance ist aus Sicherheitsgründen ausschließlich über die Anmeldung zugänglich. Daher ist es notwendig, dass Sie sich wie folgt mit Benutzername und Kennwort authentifizieren.

**Voraussetzungen:** Erwerb der REDDOXX Appliance mit den gültigen Lizenzen.

1. Kopieren Sie den Inhalt der REDDOXX CD auf Ihren Rechner.
   Die Dateien können in ein beliebiges Verzeichnis kopiert werden.
2. Klicken Sie doppelt auf die Datei *rdxadmin.exe.*
   Das Anmeldefenster öffnet sich.




Abbildung: Anmeldefenster

5. *Hostname:* Geben Sie den Hostnamen ein, zu dem Sie sich verbinden möchten oder wählen Sie ihn aus der Liste aus. Die Liste enthält die bisherigen Eingaben, die Sie bereits vorgenommen haben.
6. *Benutzername:* Geben Sie *sf-admin* ein.
7. Geben Sie das *Kennwort* ein.

**HINWEIS**

Folgende Standardwerte sind bei der Auslieferung der REDDOXX Appliance eingestellt:
*Benutzername:* sf-admin und *Kennwort:* admin

7. Wählen Sie bei Realm die Option „local“ aus.

8. Wählen Sie die gewünschte *Sprache* in der Auswahlliste aus, in der Ihr Programm angezeigt werden soll.
   Die Auswahl beinhaltet die derzeit installierten Sprachen.
9. Klicken Sie auf die Schaltfläche OK.
   Das Anwendungsfenster für die Grundkonfiguration ist jetzt aktiv.

Folgendes Anwendungsfenster beinhaltet die Bereiche der Administrator-Konsole nummeriert und benannt:

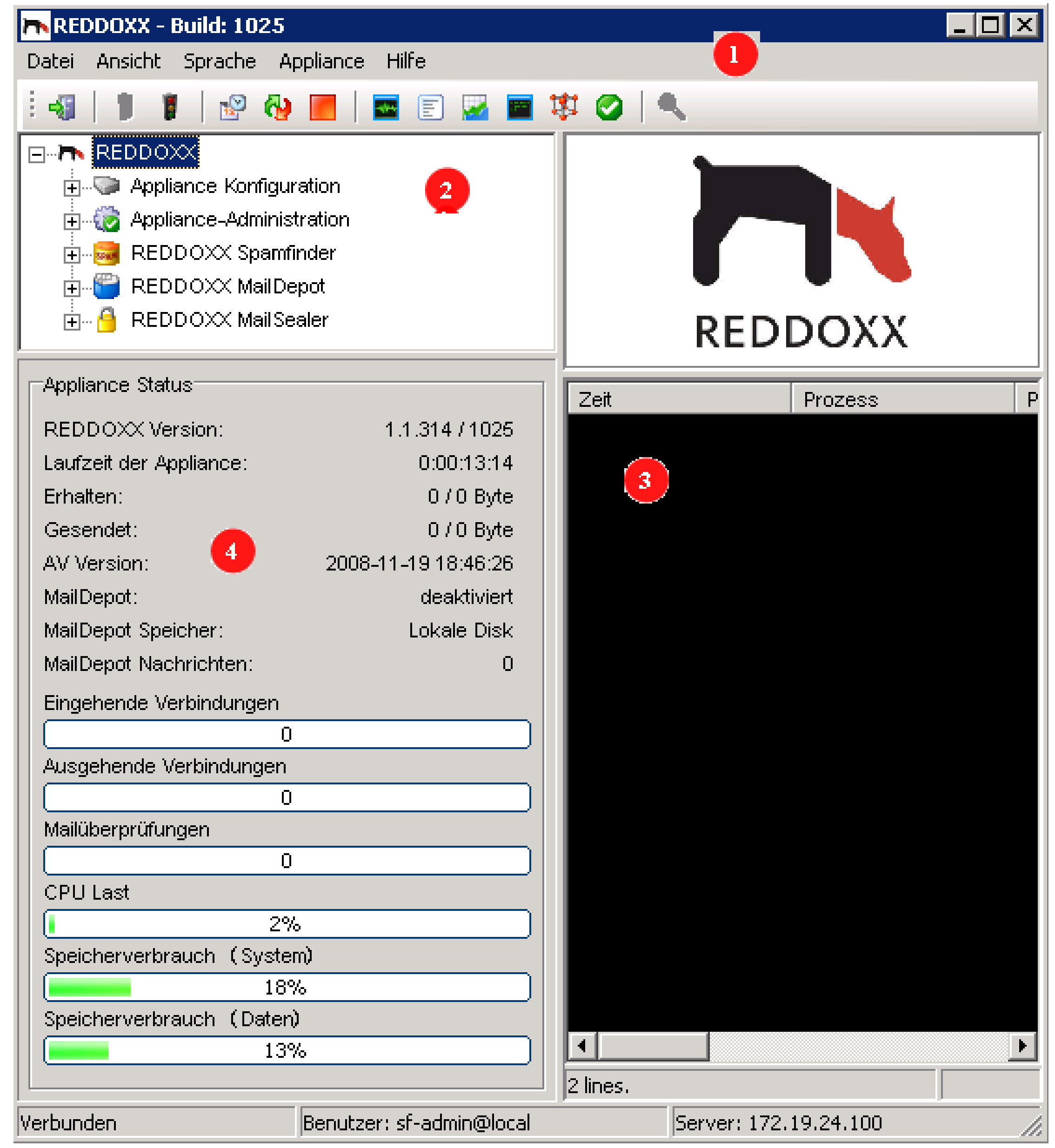


Abbildung: Anwendungsfenster nach dem Anmelden

## Legende

1. Menüleiste
2. Baumansicht
3. Listenansicht
4. Statusansicht
5. Protokollansicht

## 4.1 Optionen in der Menüleiste

Das Hauptmenü besteht aus den Bereichen Datei, Ansicht, Sprache, Appliance und Hilfe.




Abbildung: Hauptmenü

In der Titelleiste wird die Konsolenversion angezeigt. Achten Sie darauf, auch immer die aktuellste Konsolensoftware zu verwenden. Download unter http://support.reddoxx.net.

### 4.1.1 Datei - An- und Abmeldung am System

Die REDDOXX Appliance ist aus Sicherheitsgründen ausschließlich über die Anmeldung zugänglich. Daher ist es notwendig, dass Sie sich mit Benutzername und Kennwort authentifizieren.




Abbildung: Menü Datei

#### 4.1.1.1 Anmeldung ausführen (Verbinden)

**Voraussetzungen:** Die Administrator-Konsole (das Programm rdxadmin.exe) muss gestartet sein. Es besteht keine aktuelle Verbindung zum System (abgemeldet).

1. Klicken Sie im Hauptmenü *Datei* auf *Verbinden*.
   folgender Dialog wird angezeigt:




Abbildung: Anmeldefenster

8. *Hostname:* Geben Sie den Hostnamen ein, zu dem Sie sich verbinden möchten oder wählen Sie ihn aus der Liste aus. Die Liste enthält die bisherigen Eingaben, die Sie bereits vorgenommen haben.
9. *Benutzername:* Geben Sie *sf-admin* ein.
10. Geben Sie das *Kennwort* ein.

**HINWEIS**

Folgende Standardwerte sind bei der Auslieferung der REDDOXX Appliance eingestellt: *Benutzername:* sf-admin und *Kennwort:* admin

8. Wählen Sie bei Realm die Option „local“ aus.
10. Wählen Sie die gewünschte *Sprache* in der Auswahlliste aus, in der Ihr Programm angezeigt werden soll.
    Die Auswahl beinhaltet die derzeit installierten Sprachen.
11. Klicken Sie auf die Schaltfläche OK.
    Das Anwendungsfenster für die Grundkonfiguration ist jetzt aktiv.

#### 4.1.1.2 Abmeldung ausführen (Trennen)

Wenn Sie sich an einer anderen REDDOXX Appliance anmelden möchten, müssen Sie sich zunächst von der aktuellen Verbindung trennen.

1. Klicken Sie in der Menüleiste auf *TRENNEN*.
2. Schließen Sie die Anwendung (Beenden) oder melden Sie sich erneut an.

#### 4.1.1.3 Programm beenden (Beenden)

Um die Administrator-Konsole zu beenden, wählen Sie den Menüpunkt Beenden. Dabei wird auch eine evt. noch bestehende Verbindung geschlossen.

### 4.1.2 Ansicht




Abbildung: Menü Ansicht

#### 4.1.2.1 Suche

Mit der Option *SUCHE* blenden Sie im rechten oberen Fensterbereich das Sucheingabefeld ein oder aus. Sie können damit in allen Warteschlangen die Einträge nach Absender oder Empfänger durchsuchen

**Voraussetzung:** Der Inhalt einer Warteschlange oder die Archiv-Liste wird angezeigt.

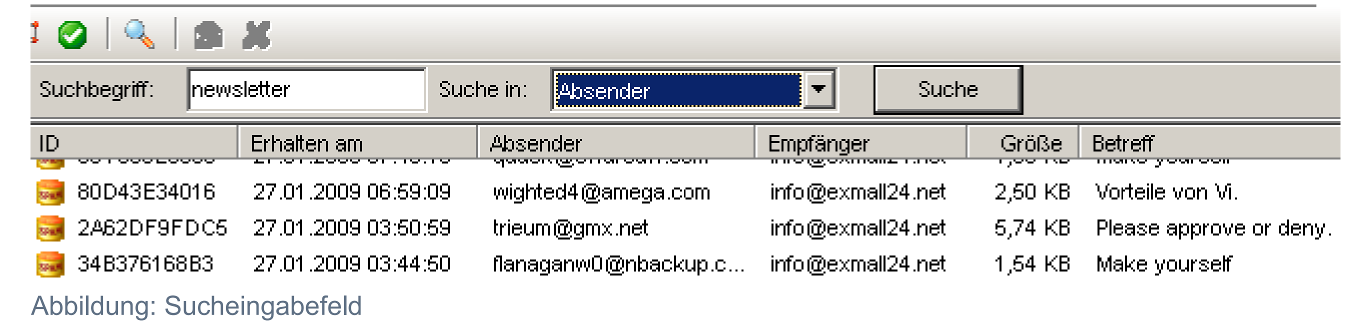



Abbildung: Sucheingabefeld

1. *Suchbegriff*: Geben Sie das Kriterium ein nach dem Sie suchen möchten.

   **HINWEIS**

   Die Anzeige wird standardmäßig auf 1000 Einträge begrenzt. Geben Sie ein „@“ ein, um sich alle Einträge anzeigen zu lassen.

2. *Suche in:* Wählen Sie in der Auswahlliste den gewünschten Feldtyp aus. Zur Auswahl stehen „Ab*sender*“ (Vorauswahl) und *„Empfänger“.*
3. *Suche*: Klicken Sie auf *SUCHE*, um die Suche zu starten.

#### 4.1.2.2 Protokoll

Über die Option *Protokoll* (auch F7-Taste) können Sie das „Live-Log-Protokoll ein- oder ausschalten. Im ausgeschalteten Modus haben Sie somit mehr Platz für die darüberliegende Listenansicht.

#### 4.1.2.3 Status

Über die Option *Status* (auch F8-Taste) können Sie die Appliance Statusanzeige im linken unteren Fensterbereichein- oder ausschalten. Im ausgeschalteten Modus haben Sie somit mehr Platz für den darüber liegenden Navigationsbaum.

#### 4.1.2.4 Statistik

Über die Statistik können Sie Diagramme über das Filterverhalten der REDOXX Appliance erstellen, drucken und speichern.
**Voraussetzung:** Protokolle müssen vorhanden sein.

1. Klicken Sie in der Menüleiste auf Ansicht.
2. Wählen Sie in der Auswahlliste den Eintrag **Statistik**.
   Folgende Ansicht wird angezeigt:

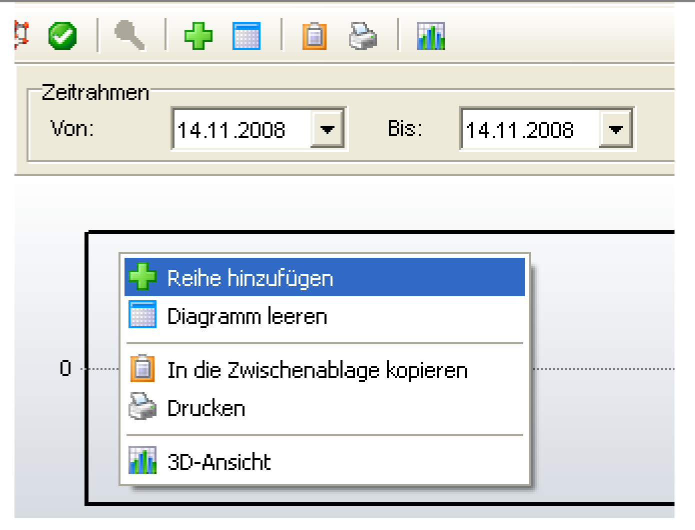



Abbildung: Statistik Kontext Menü

3. Fügen Sie mit *„Reihe hinzufügen“* einen neuen Indikator hinzu, indem Sie mit der rechten Maustaste in das Diagramm klicken.

   Folgende Ansicht wird angezeigt:

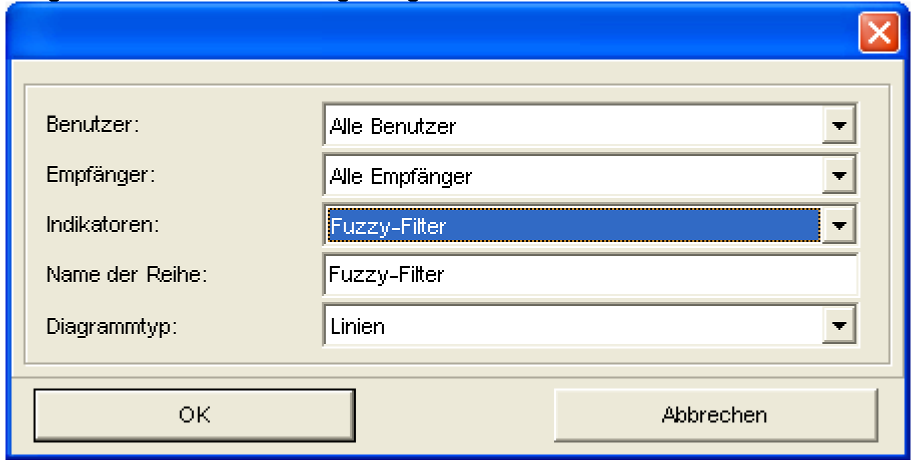



Abbildung: Reihe hinzufügen

4. Nehmen Sie die gewünschten Einstellungen vor.
5. Fügen Sie die gewählte Statistik durch Klick auf den OK Button hinzu.
   Folgende Ansicht wird angezeigt:

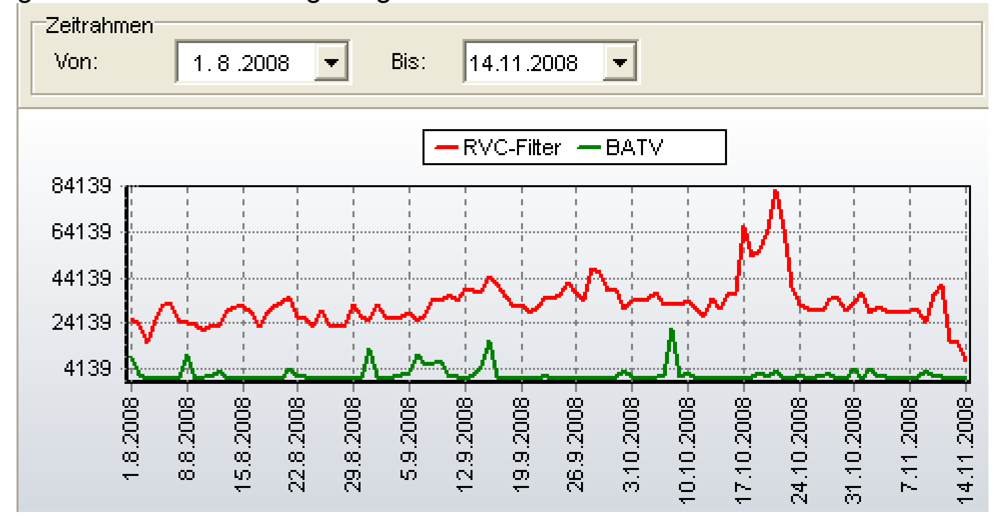


Abbildung: Statistik Diagramm

6. Klicken Sie rechts auf das Diagramm um das Kontextmenü erneut zu öffnen.
7. Wählen Sie eine andere Farbe für den Graphen.
8. Entfernen Sie den markierten Graphen.

#### 4.1.2.5 Log Viewer starten

Mit dem Log Viewer können Sie die Protokolle anschauen. Dies entspricht der gleichen Funktion wie im Kapitel Error: Reference source not found beschrieben, jedoch können Sie hiermit auch bereits lokal abgespeicherte Protokolle, oder Protokolle von anderen REDDOXX Appliances (z.B. Tochterunternehmen) sich anzeigen lassen. Öffnen Sie dazu den Dialog Datei und laden Sie die gewünschte Protokoll-Datei.

#### 4.1.2.6 CISS Manager

##### 4.1.2.6.1 CISS konfigurieren - Themen erstellen

Hier bestimmen Sie das Erscheinungsbild (Layout) Ihrer CISS-Portalseite. Wenn Sie für verschiedene Domänen unterschiedliche Layouts wünschen, erstellen Sie dazu separate THEMES und ordnen Sie die jeweilige Domäne einem Theme zu.

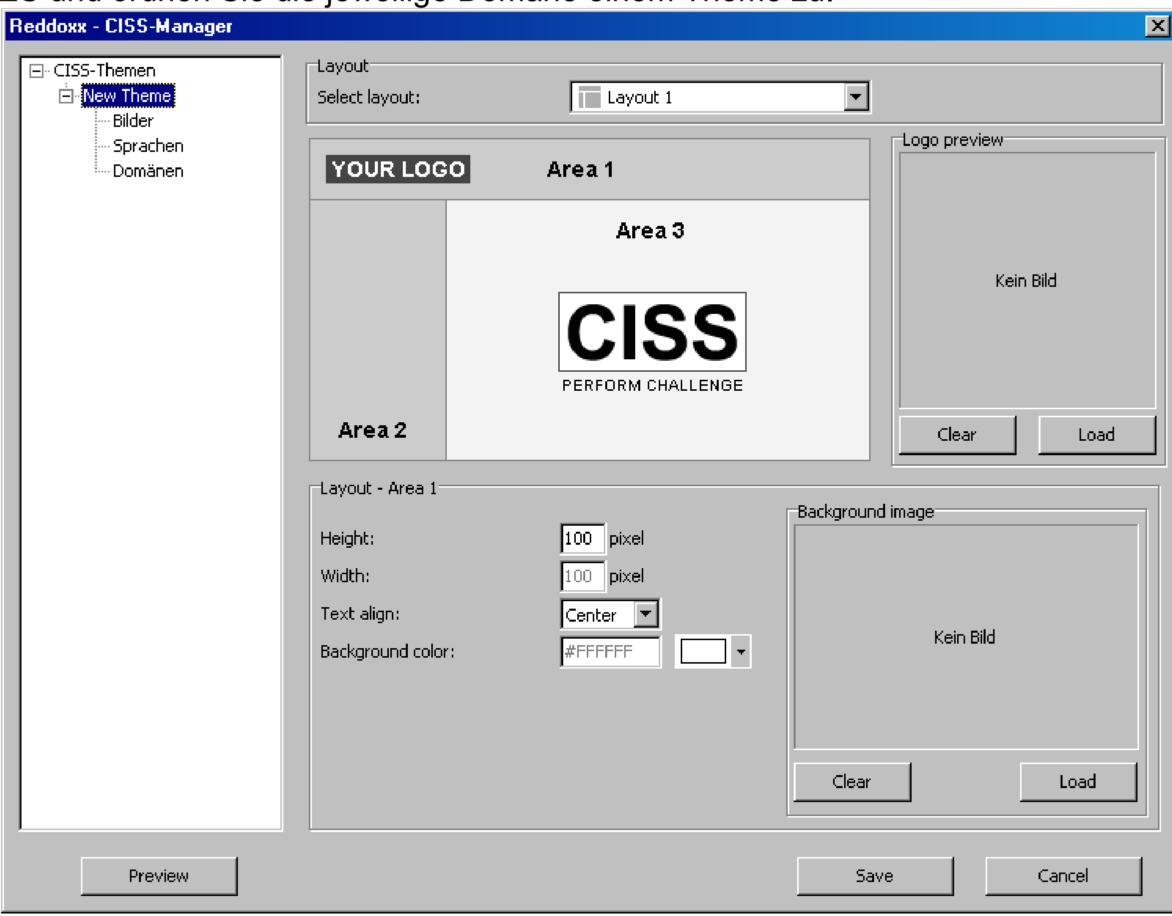



Abbildung: CISS-Manager

1. Klicken Sie im Baum mit der rechten Maustaste auf *CISS-Themen.*
2. In der Auswahlliste klicken Sie auf **Add theme** und vergeben einen Namen Ihrer Wahl.

3. Wählen Sie ein gewünschtes Layout Ihrer CISS-Seite aus. Es stehen Ihnen 5 verschiedene Layouts zur Verfügung.
4. Wählen Sie dann die einzelnen Bereiche der Seite (Area) um das entsprechende Layout zu definieren.
5. Um ein Logo einzubinden, klicken Sie auf den Button LOAD in der *Logo Preview*. Es werden die Bildformate GIF und JPG unterstützt.

**HINWEIS**

Bildgröße: 400px Breit. Größere Bilder werden automatisch verkleinert (heruntergerechnet), kleinere Bilder werden nicht vergrößert.

6. Um ein Hintergrundbild einzubinden, klicken Sie auf den Button LOAD bei *Background Image*. Es werden die Bildformate GIF und JPG unterstützt.

**HINWEIS**

Sie können ständig eine Vorschau Ihrer erstellten CISS-Seite erhalten. Klicken Sie hierzu auf den Button PREVIEW.

#### 4.1.2.6.2 CISS konfigurieren – Bilder hinzufügen

Hier können Sie Bilder für die Verwendung von CISS hinzufügen und konfigurieren.

1. Klicken Sie im Baum auf Ihr erstelltes Theme und klicken Sie danach mit der rechten Maustaste auf *Bilder*. In der Auswahlliste klicken Sie auf ***Bild hinzufügen*** und wählen Sie Ihr gewünschtes Bild aus.
   Folgende Ansicht wird angezeigt:

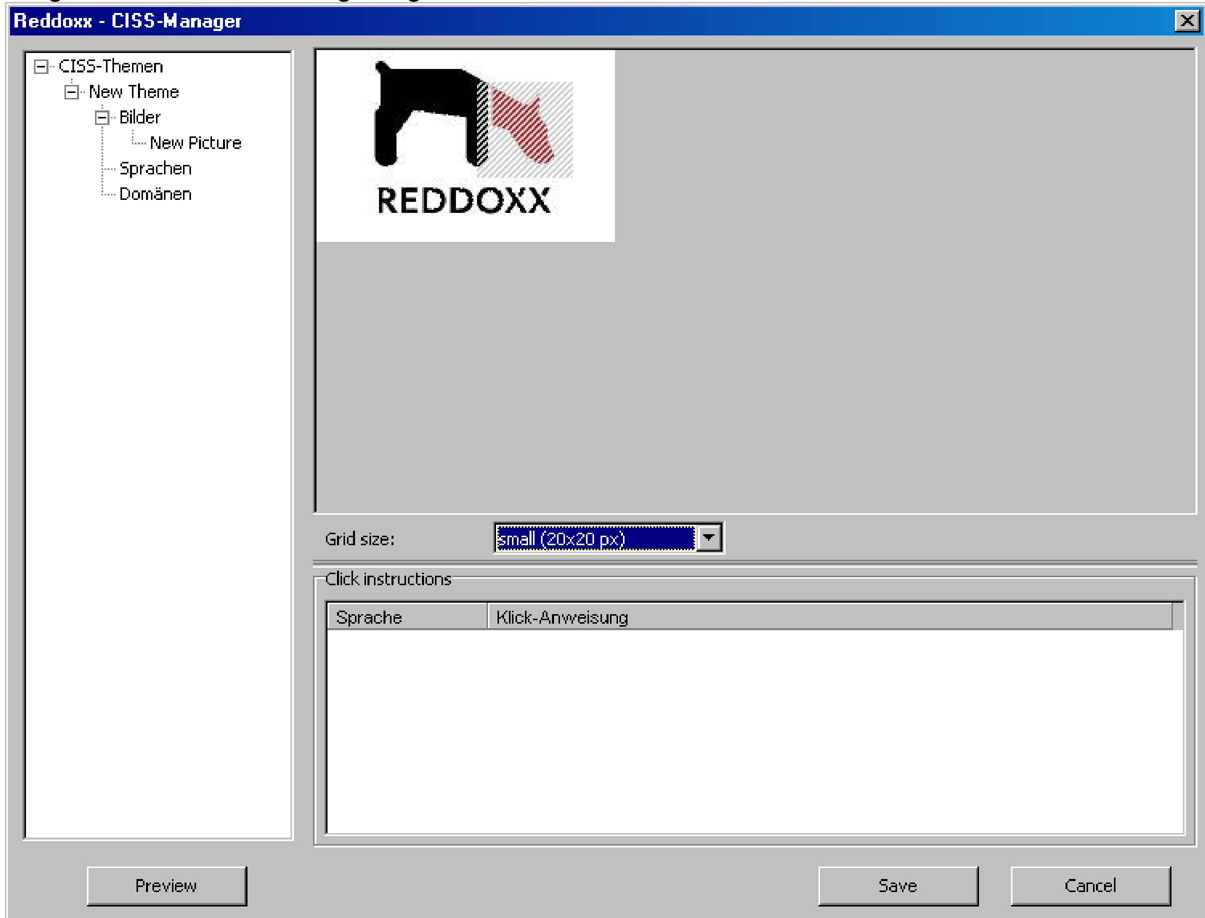



Abbildung: CISS-Manager – Bilder

2. Wählen Sie die Rahmengröße zur Erstellung der Interaktionsfelder über die Option „*Grid size*“. Definieren Sie nun die Interaktionsfelder durch Anklicken der gewünschten Bildbereiche.

**HINWEIS**

Interaktive Felder werden schraffiert markiert. Nochmaliges Klicken auf ein bereits schraffiertes Feld hebt die Interaktion wieder auf.

3. Um die Klick-Anweisungen konfigurieren zu können, müssen zuerst Sprachen hinzugefügt werden.

### 4.1.2.6.3 CISS konfigurieren – Sprachen hinzufügen

Hier können Sie verschiedene Sprachen für die Verwendung von CISS hinzufügen und konfigurieren.

1. Klicken Sie im CISS-Navigations-Baum auf Ihr erstelltes Theme und klicken Sie danach mit der rechten Maustaste auf *Sprachen*. In der Auswahlliste klicken Sie dann auf ***Sprachen hinzufügen*** und wählen Sie die gewünschte Sprache aus.
   Folgende Ansicht wird angezeigt:

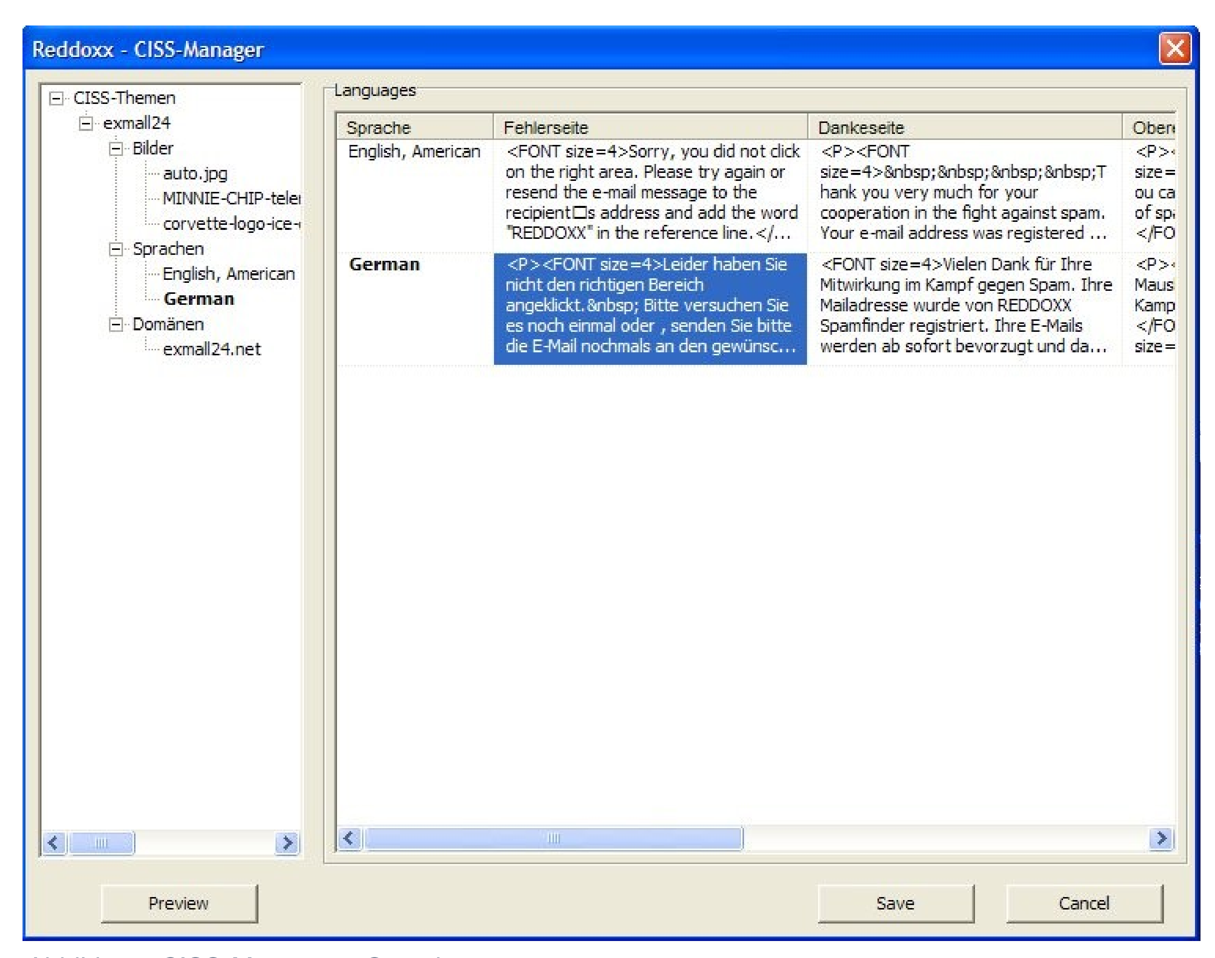



Abbildung: CISS-Manager – Sprachen

2. Sie können nun bei jeder Sprache separate Textversionen für die Parameter „Fehlerseite, Dankeseite, Oberer Text, Zurück-Button und Fenster schließen“ definieren.

3. Um diese Texte zu definieren, klicken Sie bitte doppelt auf die entsprechenden Parameter (z.B. Fehlerseite). Der Texteditor wird angezeigt:

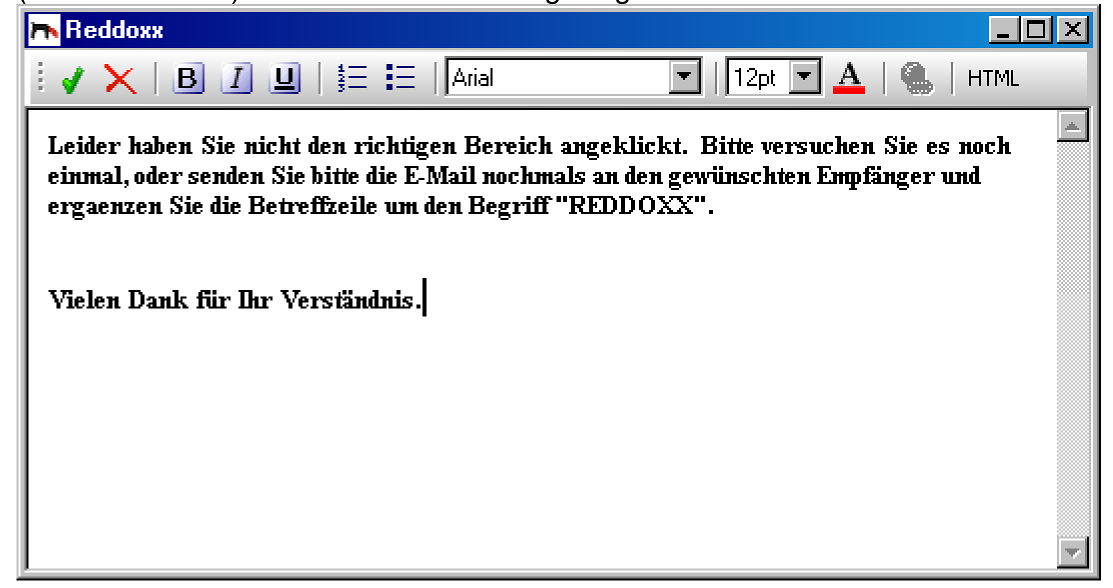



Abbildung: CISS-Manager – Sprachen - Texteditor

4. Im Texteditor können Sie Ihre eigenen Texte definieren.

**HINWEIS**

Eine Auswahl an deutschen und englischen Beispieltexten erhalten Sie im REDDOXX Support Center unter: http://support.reddoxx.net in der Rubrik REDDOXX Spamfinder – CISS - Textvorschläge.

#### 4.1.2.6.4 CISS konfigurieren – Domänen hinzufügen

Hier können Sie dem CISS-Theme eine E-Mail-Domäne zuordnen, die dann für die Verwendung von CISS aktiv ist.

**Voraussetzung:** Eine lokale Internetdomäne muss bereits konfiguriert sein.

1. Klicken Sie im Baum auf Ihr erstelltes Theme und klicken Sie danach mit der rechten Maustaste auf *Domänen*. In der Auswahlliste klicken Sie auf **Add Domain** und wählen Sie die gewünschte Domäne aus.
   Folgende Ansicht wird angezeigt:

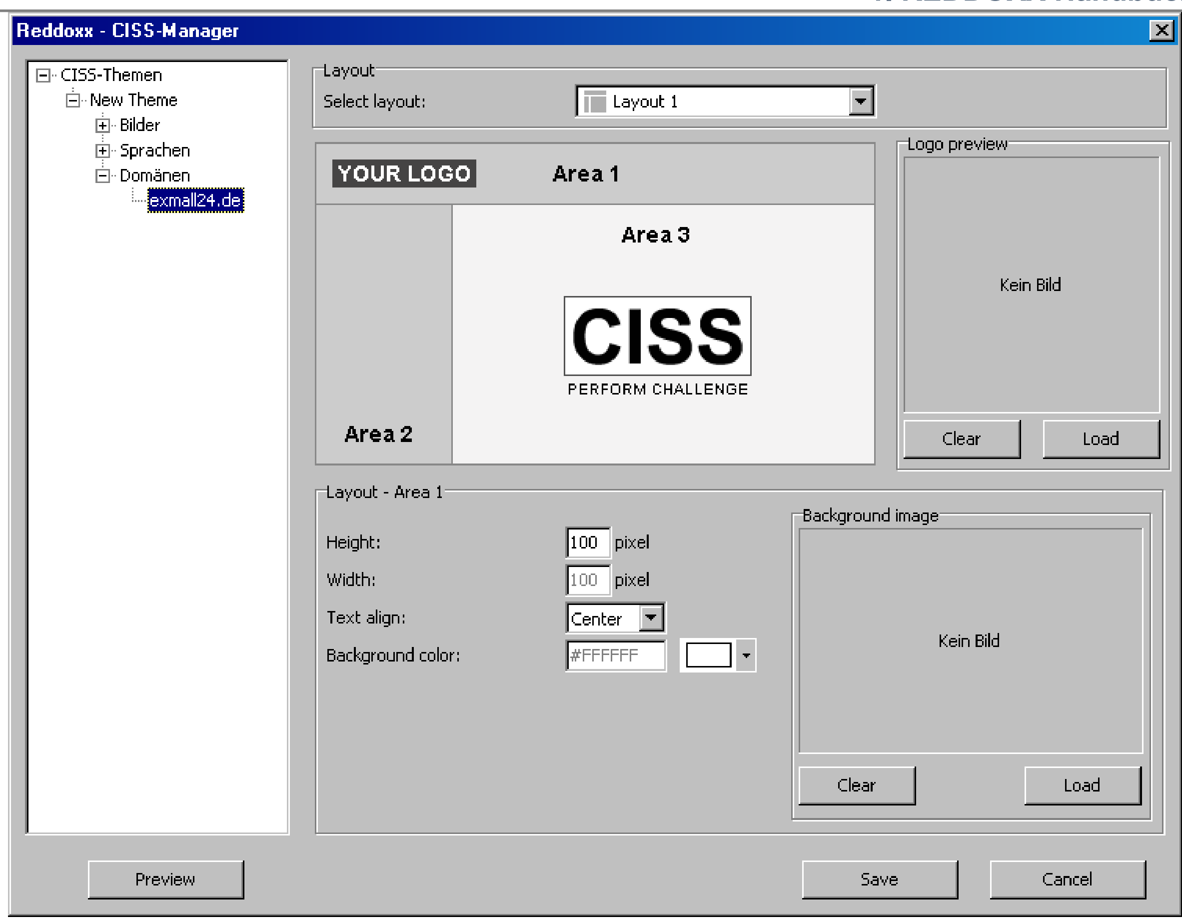



Abbildung: CISS-Manager – Domänen

**HINWEIS**

Alle unter *Domänen* eingetragenen E-Mail-Domänen sind für die Verwendung von CISS aktiviert. Damit CISS aber auch greift, muss für das jeweilige Filterprofil der CISS-Filter zugeordnet sein.

2. Um die gesamte CISS-Konfiguration zu speichern, klicken Sie bitte auf den Button SAVE. Mit Klick auf den Button CANCEL wird der CISS-Manager geschlossen und die getätigte Konfiguration verworfen.

#### 4.1.2.7 Cluster Manager

Der Cluster Manager ermöglicht das Einrichten eines Failover Clusters mit 2 Appliances. In einem Failover-Cluster übernimmt der aktive Knoten - zusätzlich die Failover IP Adresse auf seine Netzwerkkarte. Fällt der aktive Knoten aufgrund einer Störung aus, übernimmt der sekundäre Knoten die Failover IP Adresse, wird dadurch zum aktiven Knoten und ist

für die anderen Netzwerkkomponenten wie z.B. Firewall und Mail Server weiterhin unter dieser IP-Adresse erreichbar. Eine Umkonfiguration der IP-Adresse entfällt.

**Funktionsdiagramm**

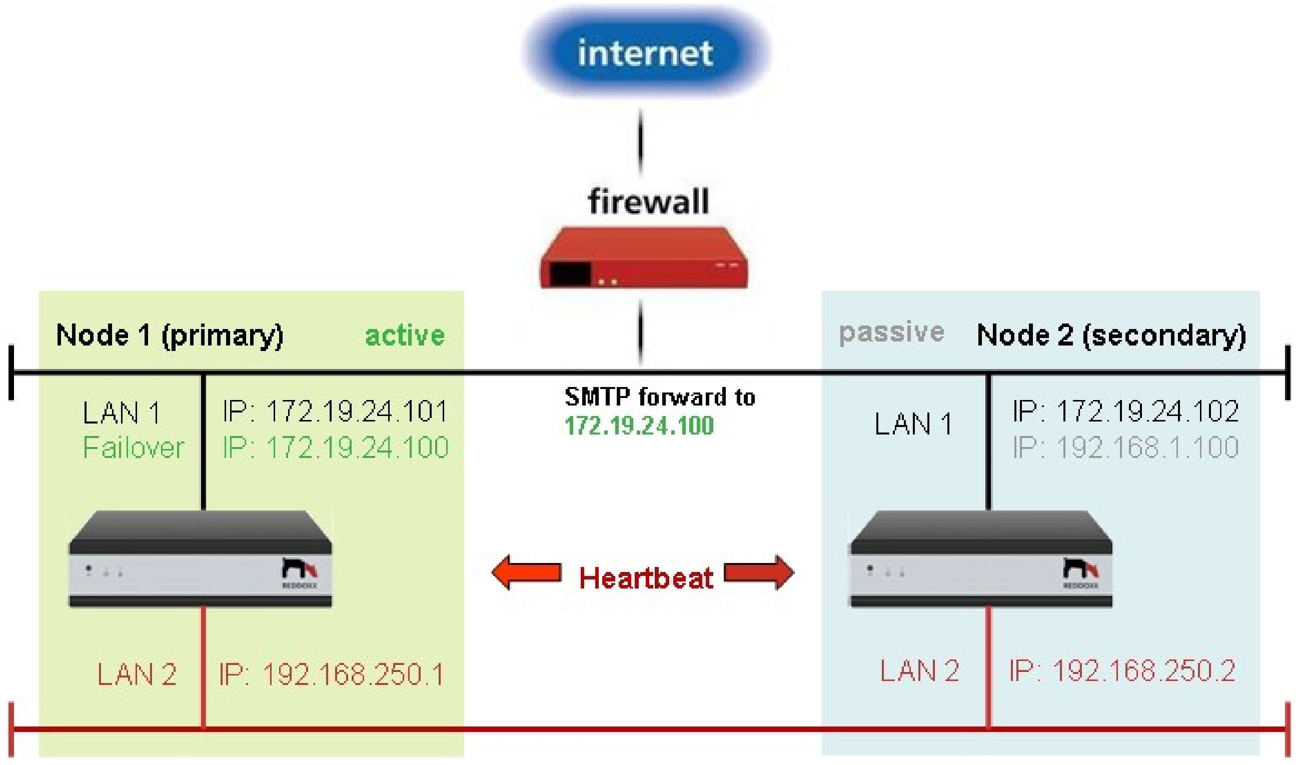



Abbildung: Cluster Funktionsdiagramm

**INFO**

Das Heartbeat Netzwerk wird über die beiden sekundären LAN-Interfaces (LAN 2) der Appliances mittels eines gekreuzten Patchkabels hergestellt. Beide Appliances überwachen mit einem regelmäßigen Impuls (Heartbeat), ob die andere Appliance noch ordnungsgemäß reagiert. Falls die primäre Appliance nicht mehr reagiert, übernimmt die sekundäre Appliance alle Datenressourcen und startet die erforderlichen Dienste (Engine und Datenbank). Im Falle einer Ressourcenübernahme (Failover) oder bei Ausfall einer Appliance erfolgt eine Benachrichtigung an den Administrator.

**Voraussetzungen**

- Zwei Reddoxx-Appliances der gleichen Produktfamilie
- Ein Ethernet-CrossOver-Kabel
- 1 Clusterlizenz passend zur Produktfamilie (Lizenz für den Clusterbetrieb).
- Eine Cluster-Subscriptions-Lizenz passend zur Produktfamilie (Lizenz zur Clusterwartung).

**Einschränkungen**

- Auf virtuellen Appliances kann das Cluster nicht während des Testbetriebes eingerichtet werden.

- Eine virtuelle Appliance muss vor dem Clusterbetrieb lizenziert sein.
- Clusterbetrieb im Bridge-Mode ist **nicht** möglich!
- In einen Netzwerk-Segment darf es nur einen REDDOXX-Cluster geben.

**Vorbereiten der Appliances**

- Beide Appliances benötigen eine vollständige Netzwerkkonfiguration.
- Während der Clusterinstallation benötigen beide Appliances Internetzugang.
- Die Datenpartition der sekundären Appliance muss gleich groß oder größer als die Datenpartition der primären Appliance sein.
- Das Kennwort für den sf-admin muss auf beiden Appliances gleich sein.
- Sie müssen auf beiden Appliances einen Zeitserver eingerichtet haben.

- Schalten Sie die IP-Adressen der beiden Appliances an der Firewall für ausgehenden Mailverkehr frei.

### 4.1.2.7.1 Einrichten des Clusterbetriebes

1. Klicken Sie in der Menüleiste auf ANSICHT -> Cluster Manager.
   Folgender Dialog wird angezeigt:




Abbildung: Cluster-Knotenauswahl

2. *Primäre Appliance:*
   Das Eingabefeld P*rimäre Appliance* ist mit dem bei der Anmeldung verwendeten Hostnamen bzw. der IP-Adresse vorbelegt.
3. *Sekundäre Appliance:*
   Geben Sie den Hostnamen oder die IP-Adresse der sekundären Appliance ein, mit der ein Cluster gebildet werden soll. Ist im Feld primäre Appliance eine IP-Adresse vorbelegt, so wird für dieses Feld diese IP-Adresse, ohne das letzte Oktett, vorgeschlagen.
4. Klicken Sie auf „Verbinden“.
   Folgender Dialog wird angezeigt:

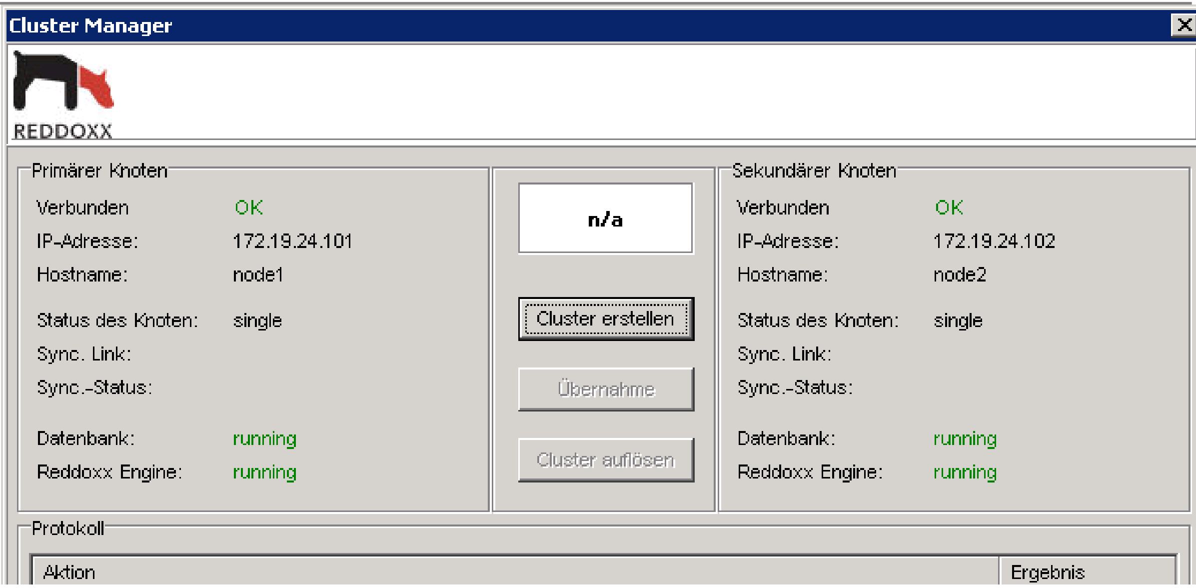


Abbildung: Cluster-Manager

5. Klicken Sie auf „Cluster erstellen".
   Folgender Dialog wird angezeigt:



Abbildung: Cluster erstellen

6. *Failover IP-Adresse:*
   Die Failover-IP-Adresse ist die IP-Adresse, über die das Cluster angesprochen wird. Es ist die Adresse, die auch auf der Firewall und auf dem Mailserver konfiguriert ist.

**HINWEIS**

Nach der Clustereinrichtung ist die primäre Appliance aktiv. Der *aktive* Clusterknoten hat die Failover IP-Adresse zusätzlich gebunden. Fällt der primäre Clusterknoten aus, übernimmt der sekundäre Clusterkonten die Failover IP-Adresse und startet die nötigen Dienste (Engine, Datenbank). Der Cluster ist somit immer unter derselben IP-Adresse erreichbar, unabhängig

davon, welcher Konten gerade aktiv ist. Die Daten werden während des Clusterbetriebes permanent in Echtzeit und transaktionssicher synchronisiert.

**Heartbeat Netzwerk**

7. *IP des 1. Knoten:*
   Standardwert: 192.168.250.1
8. *IP des 2. Knoten:*
   Standardwert: 192.168.250.2

**HINWEIS**

Das Heartbeat Netzwerk steht standardmäßig auf voreingestellte Werte. Ändern Sie die Konfiguration des Heartbeat-Netzwerkes, falls die Voreinstellungen mit einem bestehenden Netzwerk in Ihrer Umgebung kollidieren.

9. Bestätigen Sie die Eingaben mit OK.
   Folgender Dialog öffnet sich:

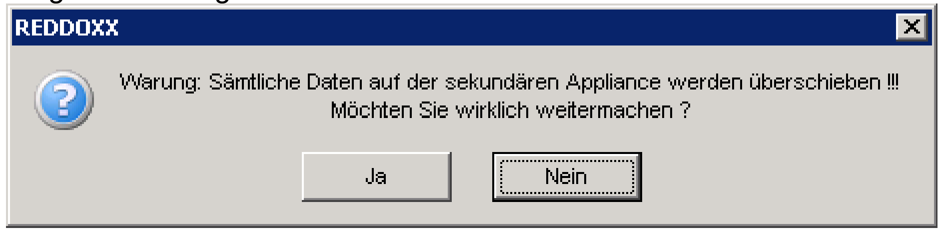



Abbildung: Sicherheitsabfrage Cluster erstellen

10. Bestätigen Sie die Sicherheitsabfrage mit „Ja“, um das Cluster jetzt einzurichten.

    Die Clustererstellung startet nun und es werden Statusmeldungen der einzelnen Schritte angezeigt. Der Vorgang dauert wenige Minuten.
    Warten Sie solange, bis ein neues Fenster mit der Meldung „Cluster erfolgreich erstellt.“ angezeigt wird.

Cluster Manager

REDDOXX

Primärer Knoten

| | |
|---|---|
| Verbunden | OK |
| IP-Adresse: | 172.19.24.101 |
| Hostname: | node1 |
| Status des Knoten: | single |
| Sync. Link: | |
| Sync.-Status: | |
| Datenbank: | running |
| Reddoxx Engine: | stopped |

n/a

Cluster erstellen

Übernahme

Cluster auflösen

Sekundärer Knoten

| | |
|---|---|
| Verbunden | OK |
| IP-Adresse: | 172.19.24.102 |
| Hostname: | node2 |
| Status des Knoten: | single |
| Sync. Link: | |
| Sync.-Status: | |
| Datenbank: | stopped |
| Reddoxx Engine: | stopped |

Protokoll

| Aktion | Ergebnis |
|---|---|
| Get version of primary node ... 1025 - 1.1.312 | OK |
| Get version of secondary node ... 1025 - 1.1.312 | OK |
| Get serial number of primary node ... 1BHR-KML2-2SKA-V2AM-YY50-74SS | OK |
| Get serial of secondary node ... 5XC3-47PD-GK6W-PS3E-LMBG-M1YT | OK |
| Get state of primary node ... | OK |
| Get state of secondary node ... | OK |
| Primary node data size: 582031 sectors | OK |
| Secondary node data size: 582031 sectors | OK |
| Register cluster with license portal ... LS72-47X0-CNZW-H943-8TY7-QWZQ | OK |
| Stop engine on primary node ... | OK |
| Stop database on primary node ... | OK |
| Stop engine on secondary node ... | OK |
| Stop database on secondary node ... | OK |
| Building secondary node configuration files ... | OK |
| Update secondary node configuration files ... | OK |
| Setup heartbeat network on secondary ... | runnning |

Idle ...

Abbildung: Protokollanzeige während der Clustererstellung

11. Wurde der Cluster erfolgreich erstellt, erscheint folgender Dialog: Bestätigen Sie mit „OK“.




Abbildung: Statusmeldung der Clustererstellung

12. Die Synchronisation der beiden Appliances beginnt. Dabei wird der Cluster-Status *gelb* angezeigt. Ist die Synchronisation fertig, wechselt der Cluster-Status auf *grün*.

**HINWEIS**

Für die nächste Anmeldung an der Admin-Konsole wird der Hostname bzw. die IP-Adresse durch die Failover-Adresse ersetzt, sodass Sie sich unabhängig davon, welcher Knoten gerade aktiv ist, am Cluster anmelden können.

13. Fügen Sie nun über den Menüpunkt „Info“ abschließend eine Cluster-Subscription Lizenz ein.

**Der Cluster-Status**

| INDIKATOR | BEDEUTUNG |
|---|---|
| Service failure | Ist das Cluster nicht betriebsbereit, wird der Status „Service failure“ in rot angezeigt. Am Ende der Clustereinrichtungs-Phase wird die Engine auf der primären Appliance neu gestartet. Dabei wechselt der Cluster-Status kurzzeitig auf *rot*. |
| Node failure | Ist eine der beiden Appliances ausgefallen oder weißt diese eine Störung auf, erscheint der Cluster-Status *orange*. |
| Synchronizing | Während der Synchronisation ist der Cluster bereits betriebsbereit, jedoch noch nicht ausfallsicher (*). Der Cluster-Status steht auf *gelb*. |
| OK | Nach erfolgreicher Synchronisation ist der Cluster nun ausfallsicher (*). Der Cluster-Status ist *grün* |

(*) *Ausfallsicher* ist in diesem Zusammenhang so definiert, dass wenn der aktive Konten ausfällt, der passive Knoten die Kontrolle übernimmt (passiv → aktiv). Weitere Maßnahmen wie z.B. Ausfall der Stromversorgung beider Appliances etc. sind hierbei nicht berücksichtigt.

### 4.1.2.7.2 Übernahme des Betriebes auf den anderen Clusterknoten

Für den Fall, dass Sie die Kontrolle auf den anderen Clusterknoten legen möchten (z.B. wegen Hardware-Wartung), können Sie das Cluster „umfallen lassen“. Die bisherige passive Appliance wechselt dabei den Status auf aktiv, die bisherige aktive Appliance wechselt auf passiv.

1. Wählen Sie im Menü „Ansicht“ den Cluster-Manager.
2. Klicken Sie auf „Übernahme“.
   Folgender Dialog öffnet sich:

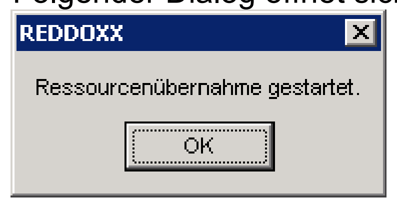



Abbildung: Bestätigung der Ressourcen-Übernahme

### 4.1.2.7.3 Aufheben des Cluster Betriebs

3. Wählen Sie im Menü *„Ansicht“* den Cluster-Manager.
4. Klicken Sie auf „Cluster auflösen“.
   Folgender Dialog öffnet sich:

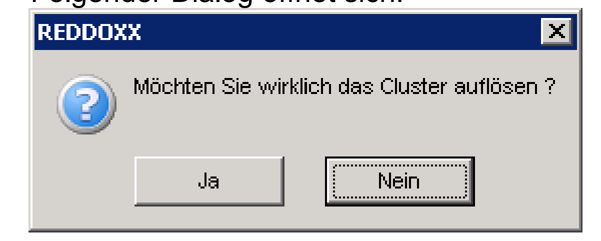


Abbildung: Sicherheitsabfrage vor der Clusterauflösung

Bestätigen Sie das Auflösen mit „Ja“.

5. Während dem Auflösen erscheinen im Protokollfenster des Cluster Managers Statusmeldungen zu den einzelnen Schritten.
Zuletzt erscheint folgender Dialog:

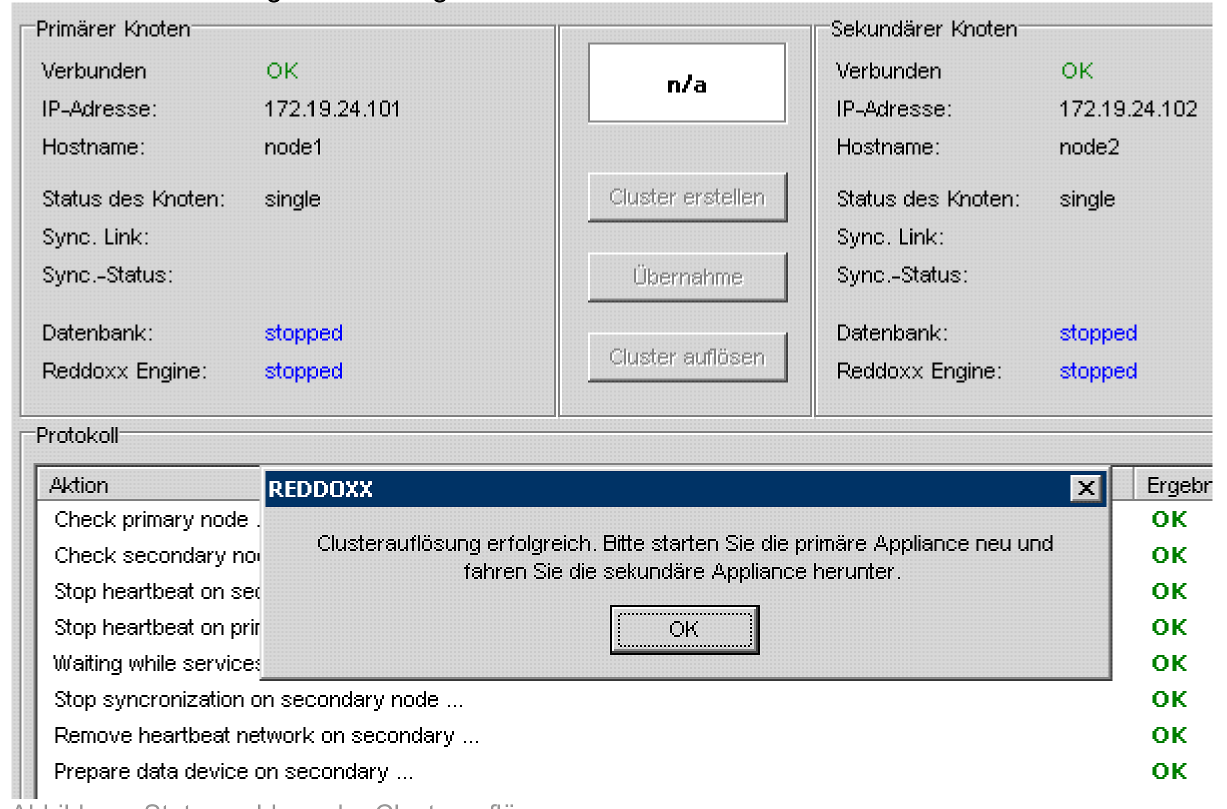



Abbildung: Statusmeldung der Clusterauflösung

**HINWEIS**

Nach dem Auflösen des Cluster-Betriebes haben beide Appliances den gleichen Datenbestand. Daher sollte **nur eine der beiden Appliances weiter betrieben** werden, da sonst **E-Mails**, die bereits die Appliance erreicht hatten, aber noch nicht versendet wurden, nun **doppelt versendet** werden!

Die Appliance, die Sie weiter betreiben möchten, muss **neu gestartet** werden (Reboot). Die andere Appliance sollten Sie ausschalten. Überlegen Sie, ob Sie die sekundäre Appliance **vor dem Ausschalten** auf den Auslieferungszustand zurückzusetzen möchten.

Achten Sie dabei auch darauf, dass die **Netzwerkeinstellungen**, insbesondere die IP-Adresse neu eingestellt werden müssen, so dass die Firewall und der Mailserver die Appliance korrekt adressieren können.

### 4.1.2.7.4 Aufheben des Cluster-Betriebs bei Ausfall eines Clusterkonten

Wenn eine Appliance aus dem Cluster nicht verfügbar ist (Status *Node failure*), kann das Cluster nicht geordnet aufgelöst werden. Um die verbleibende Appliance in den normalen Betriebsmodus zu versetzen, gehen Sie wie auch in Kapitel 6 beschrieben, vor.

1. Melden Sie sich direkt an der Appliance Konsole an.

**HINWEIS**

Ein Aufheben des Clusters via einer SSH-Konsolenverbindung (z.B. Putty) ist nicht möglich!

2. Wählen Sie „Cluster “ ➔„Leave Cluster“
3. Bestätigen Sie die Sicherheitsabfrage mit „Ja“.
4. Starten Sie die Appliance anschließend neu.

#### 4.1.2.7.5 Lizenzen im Cluster-Betrieb

Beim Einrichten eines Clusters werden die Lizenzen der primären Appliance in den Cluster übernommen. Sollte das Cluster zu einem späteren Zeitpunkt aufgelöst werden, sind Lizenzen, die während des Cluster-Betriebes hinzugefügt wurden, der primären Appliance automatisch zugeordnet.

**HINWEIS**

Für den Cluster-Betrieb sind eine Cluster-Lizenz und eine Cluster-Subscription erforderlich.

### 4.1.2.8 Diagnose Center

Das Diagnose Center bietet die Möglichkeit die Appliance auf vorhandene oder bevorstehende Probleme zu überprüfen. Zur Auswahl steht die Komplettdiagnose oder ein Einzel-Check.

1. Wählen Sie im Menü „Ansicht“ das „*Diagnose Center*“.
   Folgender Dialog öffnet sich:

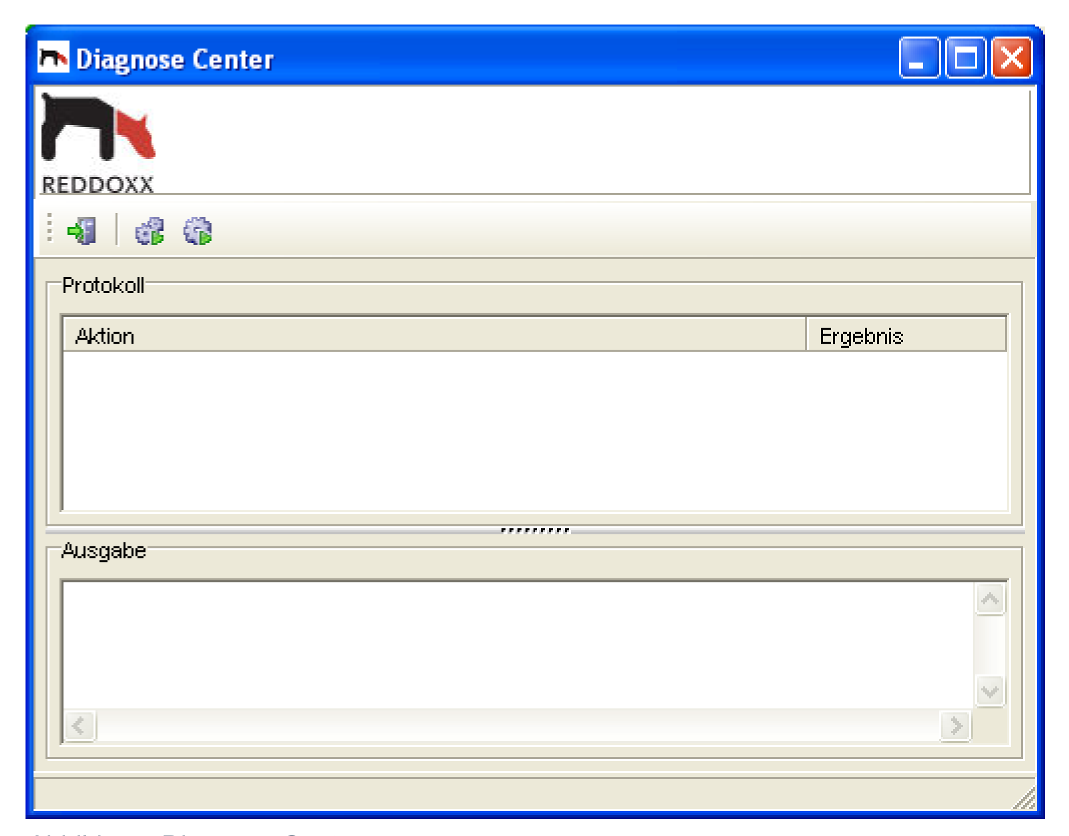



Abbildung: Diagnose Center

2. Beendet das Diagnose Center.

3. Startet eine Komplettdiagnose.
Folgender Dialog öffnet sich:

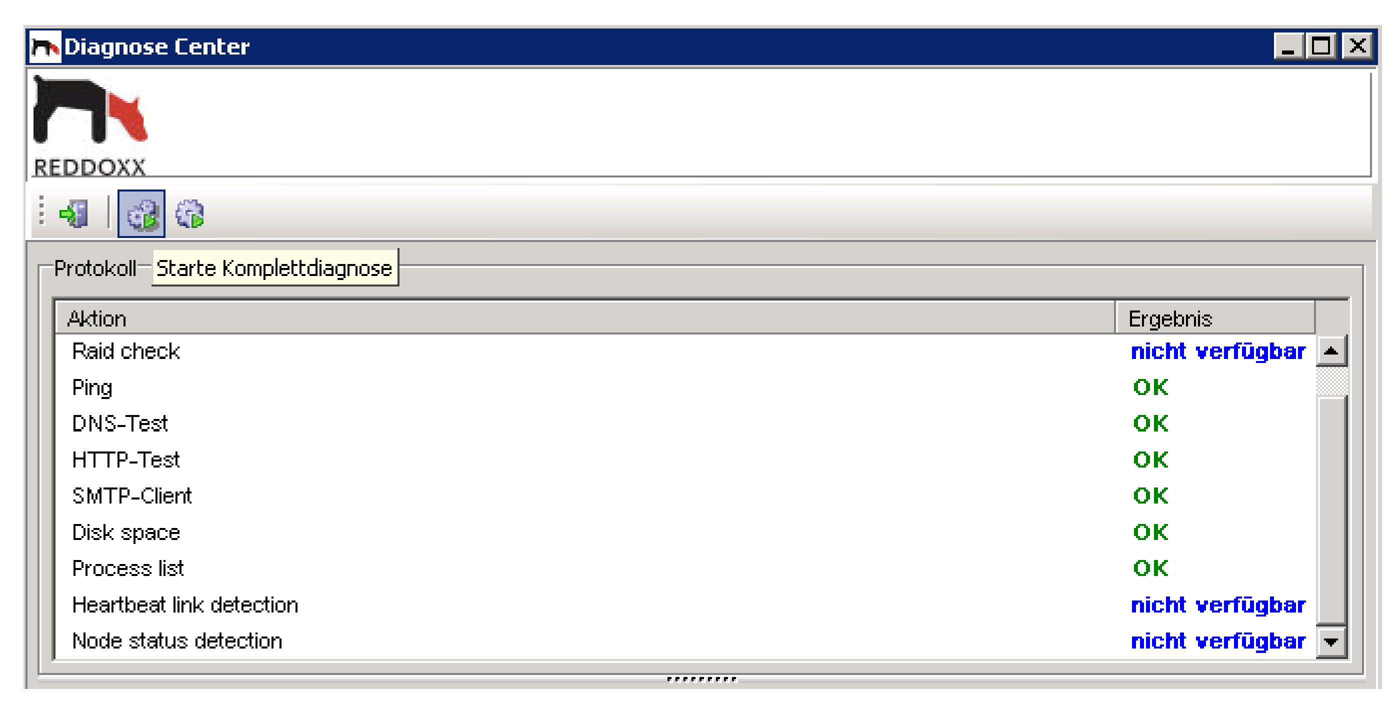



Abbildung: Komplettdiagnose

**Aktion**
Im Aktionsfenster werden nun die einzelnen Diagnoseschritte durchlaufen.

**Ausgabe**
Im Ausgabefenster sehen Sie detaillierte Informationen zu einer einzelnen Diagnose. Klicken Sie dazu auf eine gewünschte Aktion.
Sie sehen folgende Statusinformationen:

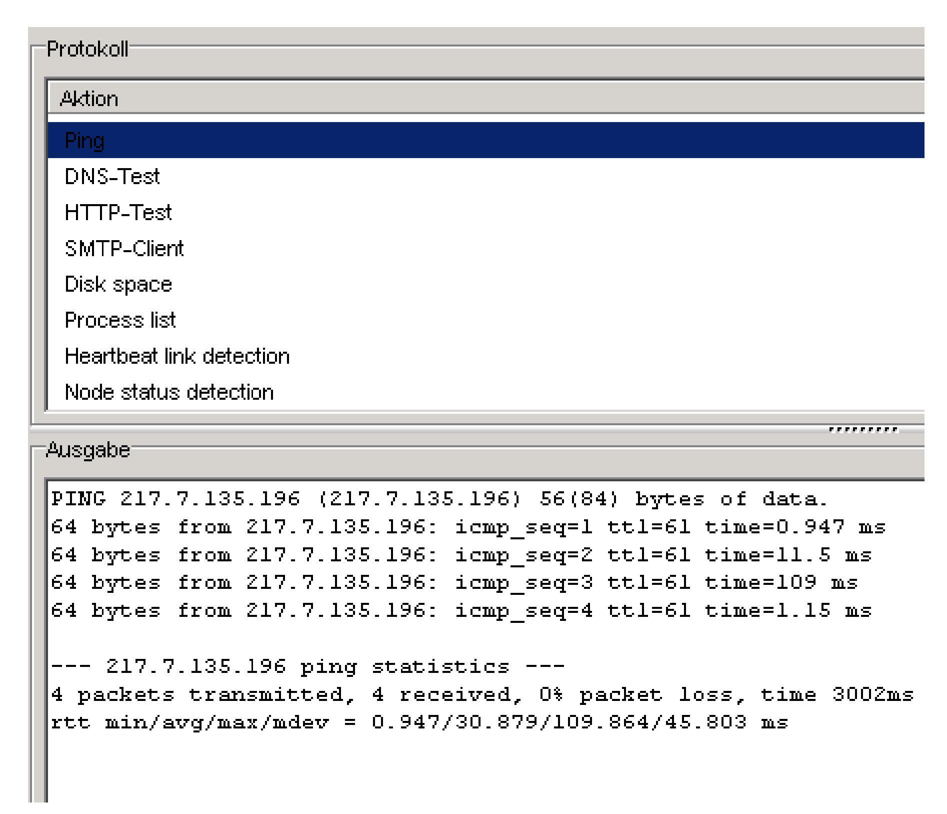



Abbildung: Statusinformationen einer Diagnose im Ausgabefenster

4. Startet eine Einzeldiagnose
Einzeldiagnosen sind in Kategorien gruppiert. Sie können alle Diagnosen einer gesamten Kategorie oder eine einzelne Diagnose ausführen.
Wählen Sie eine Kategorie aus der folgenden Auswahlliste:

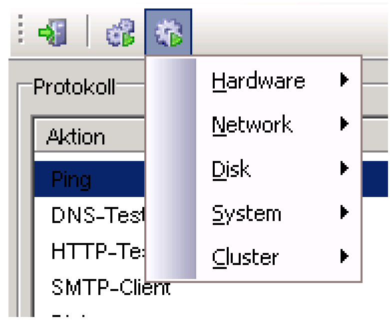



Abbildung: Diagnose-Kategorien

5. Startet eine Einzeldiagnose
Einzeldiagnosen sind in Kategorien gruppiert. Sie können alle Diagnosen einer

gesamten Kategorie oder eine einzelne Diagnose ausführen.

Wählen Sie

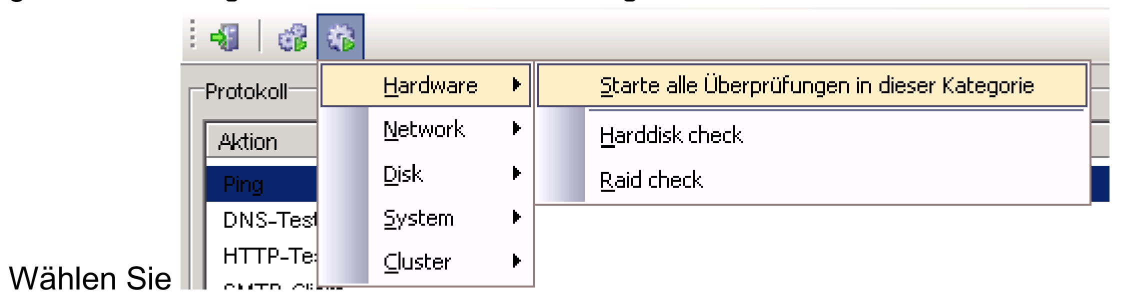



Abbildung: Auswahl einer Einzel-Diagnose

Am Ende der Diagnose erscheint eine Statusmeldung:

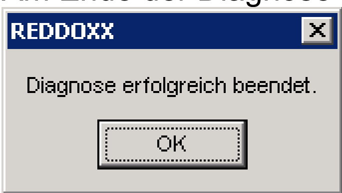



Abbildung: Diagnose Status

**HINWEIS**

Die Appliance führt jede Stunde selbstständig eine Komplettdiagnose durch. Im Falle einer Fehlererkennung wird der Administrator durch eine E-Mail benachrichtigt.

### 4.1.3 Sprache

Sie können derzeit zwischen 4 verschiedenen Sprachen wählen. Englisch, Deutsch, Holländisch und Italienisch.
Wählen Sie im Menü SPRACHE die gewünschte Sprache aus. Alle Ansichten werden sofort in der neuen Sprache angezeigt.




Abbildung: Menüpunkt Sprache

### 4.1.4 Appliance

Im Bereich Appliance können Sie die REDDOXX Appliance neu starten, ausschalten, Datum und Zeit setzen.

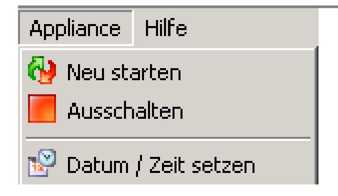



Abbildung: Menüpunkt Appliance

#### 4.1.4.1 Appliance neu starten

Hier können Sie die REDDOXX Appliance bequem über die REDDOXX Konsole neu starten.

**Voraussetzung:** Anmeldung an die REDDOXX Appliance muss bestehen.

1. Klicken Sie in der Menüleiste auf Appliance.
2. Wählen Sie in der Auswahlliste den Eintrag **Neu starten**. Die Appliance ist in ca. 1 Minute wieder betriebsbereit.

#### 4.1.4.2 Appliance ausschalten

Hier können Sie die REDDOXX Appliance bequem über die REDDOXX Konsole ausschalten.

**Voraussetzung:** Anmeldung an die REDDOXX Appliance muss bestehen.

1. Klicken Sie in der Menüleiste auf Appliance.
2. Wählen Sie in der Auswahlliste den Eintrag **Ausschalten**.

#### 4.1.4.3 Datum / Zeit setzen

Hier können Sie das Datum und die Zeit der REDDOXX Appliance mit den aktuellen Einstellungen des Computers gleichsetzen.

**Voraussetzung:** Richtige Einstellungen am Computer (BIOS).

1. Klicken Sie in der Menüleiste auf Appliance.
2. Wählen Sie in der Auswahlliste den Eintrag **Datum / Zeit setzen**.

### 4.1.5 Hilfe

Das Hilfe-Menü besteht aus den Punkten **Lizenzinformation**, **Online-Hilfe**, **REDDOXX Support Webseiten** und **Starte Remote Support**.

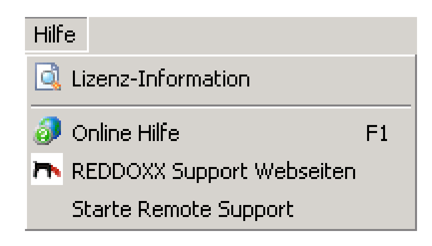



Abbildung: Menüpunkt Hilfe

### 4.1.5.1 Lizenz-Information

**Lizenz-Information anpassen**

Hier können Sie die Lizenzen für die REDDOXX Appliance verwalten.
**Voraussetzung:** Erwerb der REDDOXX Appliance.

1. Klicken Sie in der Menüleiste auf Info.
2. Wählen Sie in der Auswahlliste den Eintrag **Lizenz-Information**.
   Folgende Ansicht wird angezeigt:

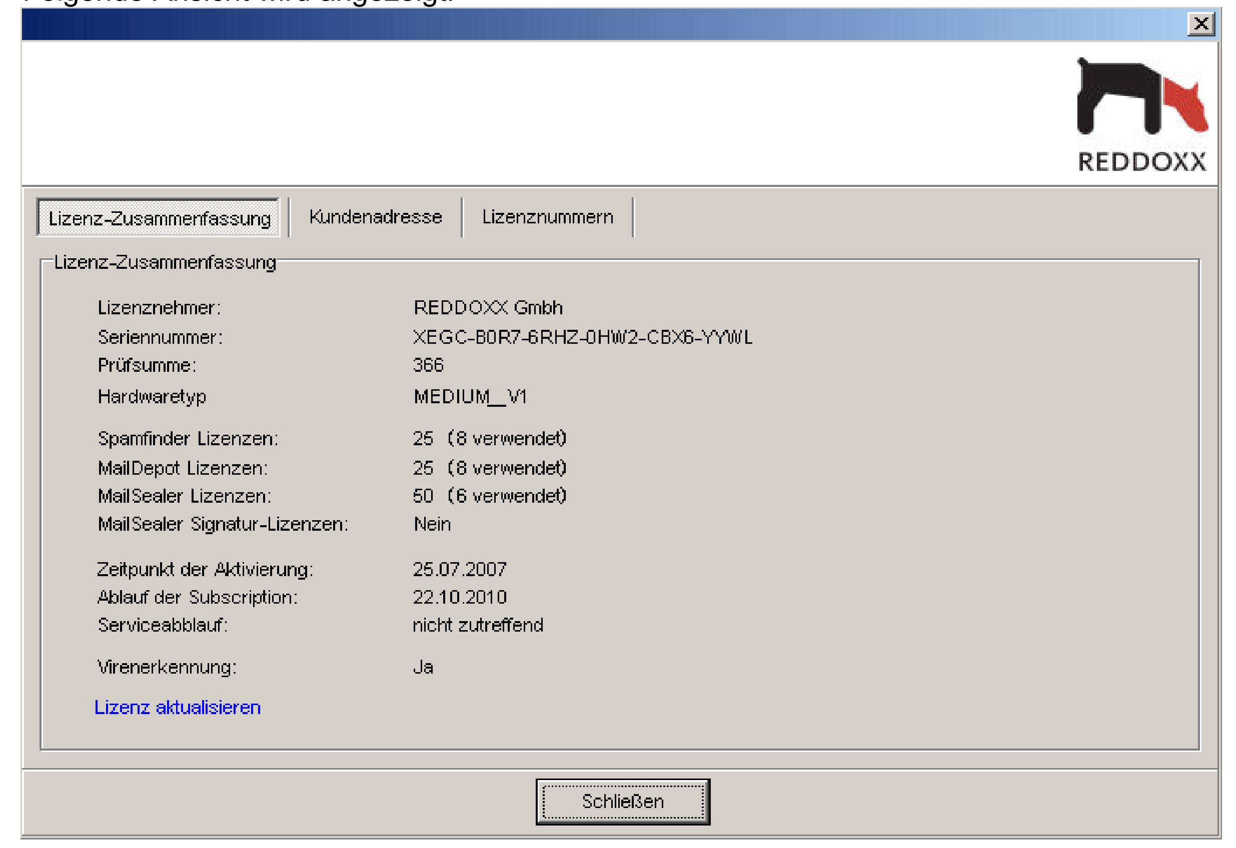



Abbildung: Lizenz Information - Lizenzzusammenfassung

3. In der Lizenzzusammenfassung erhalten Sie Informationen über den Lizenznehmer, die Lizenzanzahl und dem Ablauf der Subscription. Mit Klick auf *Lizenz aktualisieren* wird die Lizenzzusammenfassung aktualisiert.

**Kundenadresse**

Hier können Sie Ihre Adressdaten verwalten und aktualisieren.
**Voraussetzung:** Erwerb der REDDOXX Appliance.

1. Klicken Sie in der Menüleiste auf Info.
2. Wählen Sie in der Auswahlliste den Eintrag **Lizenz-Information**.
3. Klicken Sie auf den Reiter "Kundenadresse".
   Folgende Felder werden angezeigt:

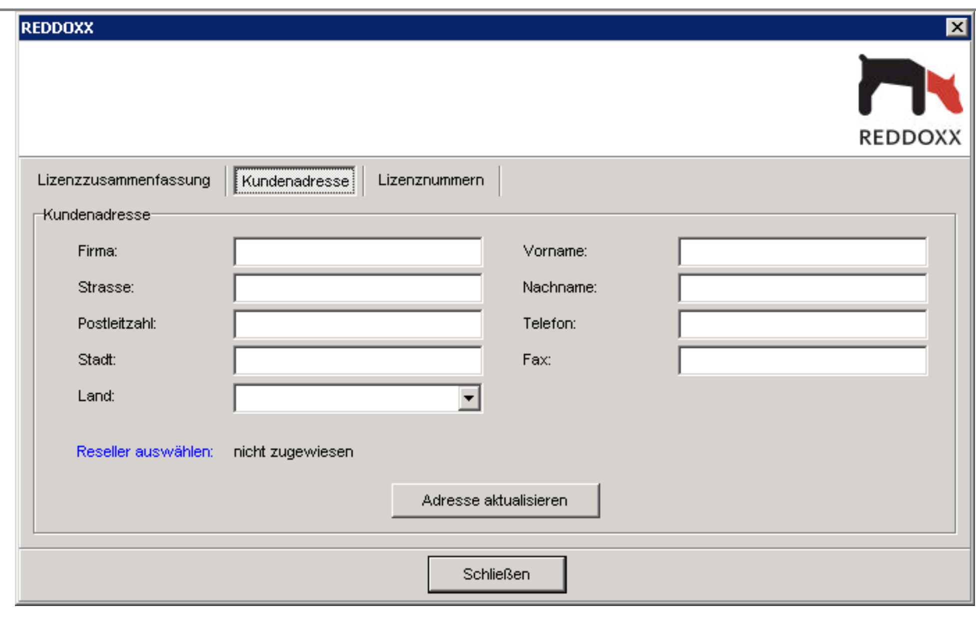



Abbildung: Lizenz Information - Kundenadresse

4. Füllen Sie alle Felder ordnungsgemäß aus und klicken Sie auf *Händler auswählen*.

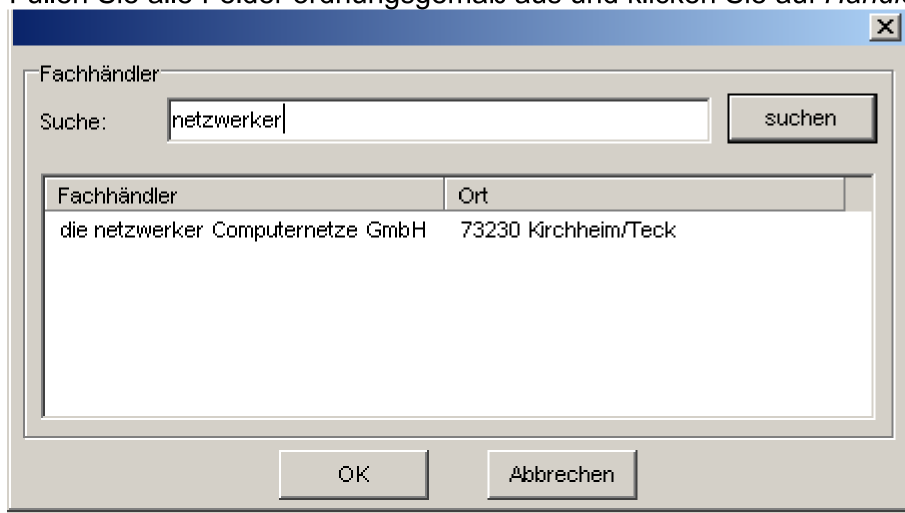



Abbildung: Lizenz Information - Fachhändlerauswahl

5. Wählen Sie Ihren Fachhändler aus. Dazu müssen Sie mindestens 4 Zeichen eingeben.
6. Klicken Sie abschließend auf *Adresse aktualisieren.*

**Lizenznummern**

Hier werden Ihre REDDOXX Lizenzen und Subscriptions verwaltet.

1. Klicken Sie auf den Reiter "Lizenznummern".
   Folgende Felder werden angezeigt:

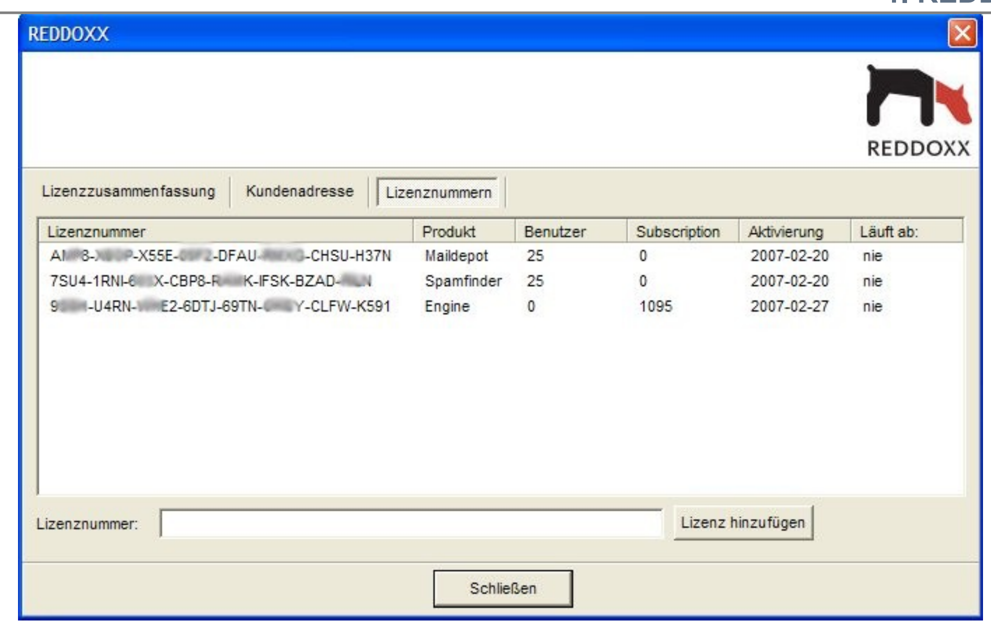



Abbildung: Lizenz Information - Lizenznummern

2. Sie sehen eine Übersicht aller eingetragenen Lizenzen mit Aktivierungs- und Ablaufinformationen.
   Um eine neue Lizenz einzutragen, geben Sie die erworbene Lizenznummer in das Feld *Lizenznummer* ein.
3. Um die eingetragene Lizenznummer auf der REDDOXX Appliance zu registrieren, klicken Sie auf den Button LIZENZ HINZUFÜGEN.

#### 4.1.5.2 Online Hilfe

Mit der Online Hilfe (F1) gelangen Sie automatisch zum Reddoxx Online Handbuch. Mit Drücken der F1-Taste wird Ihr Browser gestartet und der zum Kontext passende Hilfetext aus dem Handbuch angezeigt.

#### 4.1.5.3 REDDOXX Support

Falls Sie Fragen zur Administration haben, oder ein Problem bei REDDOXX melden wollen, können Sie über die Funktion REDDOXX Support eine Support Anfrage starten. Dabei werden Sie über Ihren Browser auf die Support-Anfrageseite von REDDOXX geleitet.

REDDOXX Support Center




HOME | DOWNLOAD | FAQ | HANDBÜCHER | ANFRAGE | DEMO-CENTER | REDDOXX.COM

**Support-Anfrage**

Sie haben Fragen zur Administration Ihrer REDDOXX Appliance oder möchten eine Störung melden? Dann füllen Sie bitte dieses Formular möglichst vollständig aus. Wir werden Ihre Anfrage umgehend bearbeiten.

Appliance Serial No.: 1BHR-KML2-2SKA-V2AM-YY50-74SS *)

Hardware Serial No.: 123456 *)

| | | | |
|---|---|---|---|
| Hardware defekt: | ☐ | Mailfluss gestört: | ☐ |
| Fragen zur Administration: | ☐ | Featurewunsch: | ☐ |

**Aktuelle Firmware**

**Release**

| | |
|---|---|
| Build: | 1025 Beta |
| Version: | 1.1.312 |

how to get / download

**Schnellsuche FAQ**

Suche Detailsuche

Abbildung: Lizenz Information - Lizenznummern

#### 4.1.5.4 Start Remote Support

Klicken Sie auf diese Schaltfläche, wenn Sie den Remotezugriff für den REDDOXX Support Mitarbeiter freischalten wollen. Die Appliance baut anschließend eine Verbindung über Port 80 zu dem Reddoxx Support Server auf. Über diese Verbindung kann sich der technische Support auf Ihre Appliance schalten und weitere Analysen vornehmen.

1. Wählen Sie aus dem Menü *Hilfe* den Punkt *Starte Remote Support* aus.
   Der Remote Support Service wird nun gestartet, es wird folgender Dialog angezeigt, den Sie mit OK bestätigen.




2. Um den Dienst wieder zu beenden, wählen Sie aus dem Menü *Hilfe* den Punkt *Stoppe Remote Support* aus.
   Der Remote Support Service wird nun wieder gestoppt, es wird folgender Dialog angezeigt, den Sie mit OK bestätigen.




## 4.2 Appliance Konfiguration

### 4.2.1 Netzwerkeinstellungen

**Netzwerkeinstellungen öffnen**

**Voraussetzungen:** REDDOXX Appliance muss angeschlossen und in Betrieb sein.

1. Klicken Sie im Navigationsbaum doppelt auf ***Appliance Konfiguration***.
2. Klicken Sie im Baum den Zweig ***Netzwerkeinstellungen*** doppelt.

**ACHTUNG**

**Sie sollten vor jeder Änderung ein Backup machen und dieses archivieren.**
**Siehe auch: "Optionen in der Menüleiste"**

### 4.2.1.1 Netzwerkeinstellungen - Allgemein

**Netzwerk Konfiguration vornehmen**

Über die Allgemeine Konfiguration können Sie den Hostname und die DNS-Server einrichten.

**Voraussetzung:** Appliance Konfiguration öffnen.

1. Klicken Sie auf den Reiter "Allgemein".
   Folgende Felder werden angezeigt:

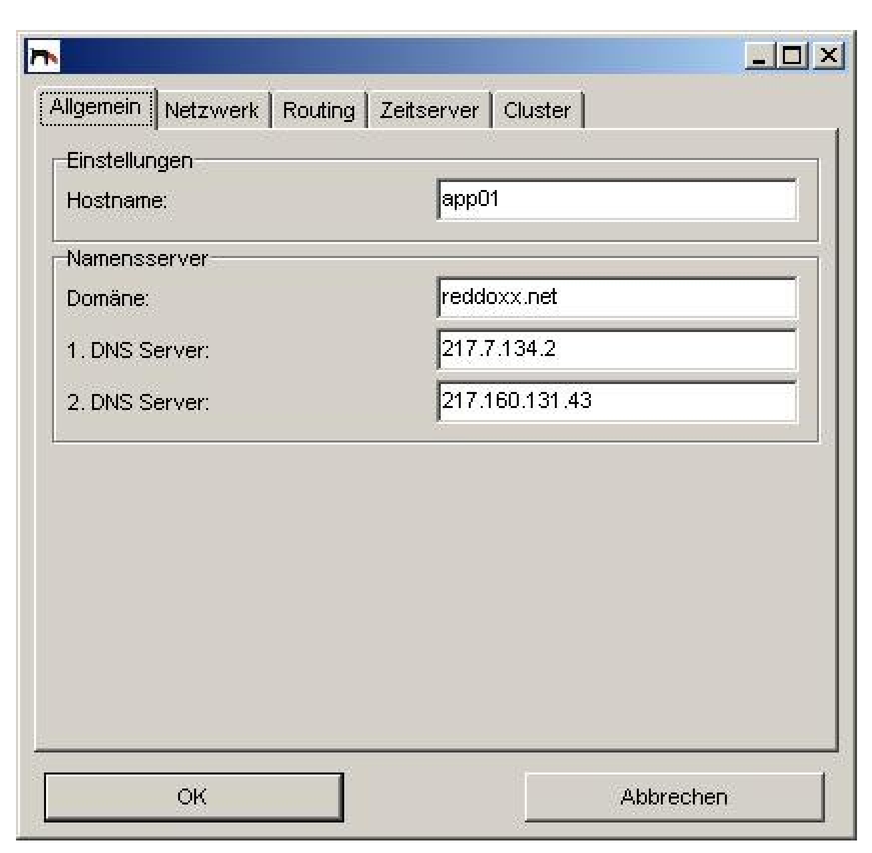



Abbildung: Allgemeine Konfiguration der REDDOXX Appliance

2. *Hostname - Hostname:*
   Geben Sie einen beliebigen Namen für die REDDOXX Appliance im Netzwerk an. Der Standardwert kann mit einem beliebigen Namen ausgetauscht werden.
3. *DNS - Domäne:*
   Geben Sie eventuell den Namen der Domäne an, welcher der REDDOXX Appliance angehört.
4. *DNS - 1. DNS-Server:*
   Geben Sie die entsprechende IP-Adresse des DNS-Servers Ihres Netzwerkes an.

**HINWEIS**

Diese Eingabe ist Pflicht! Es muss mindestens ein DNS-Server angegeben werden. Achten Sie darauf, dass der DNS-Server auch erreichbar ist, wenn Sie die REDDOXX-Appliance in einer DMZ betreiben.

5. *DNS - 2. DNS-Server:*
   Geben Sie die IP-Adresse eines weiteren DNS-Servers an.

   **HINWEIS**

   Achten Sie bei der Angabe eines zweiten DNS Servers, dass dieser auch die gleiche Datenbasis wie der erste DNS Server hat.

6. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Appliance Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Netzwerk Konfiguration.

### 4.2.1.2 Netzwerkeinstellungen - Netzwerk

**Netzwerk Konfiguration vornehmen**

Über die Netzwerk Konfiguration können Sie die erste *Netzwerkkarte* konfigurieren. Diese besteht jeweils aus einer IP-Adresse und einer Netzmaske.

**HINWEIS**

Die Konfiguration der zweiten Netzwerkkarte wird derzeit noch nicht unterstützt.

**Voraussetzung:** Netzwerk Konfiguration öffnen.

1. Klicken Sie auf den Reiter "Netzwerk".
   Folgende Felder werden angezeigt:

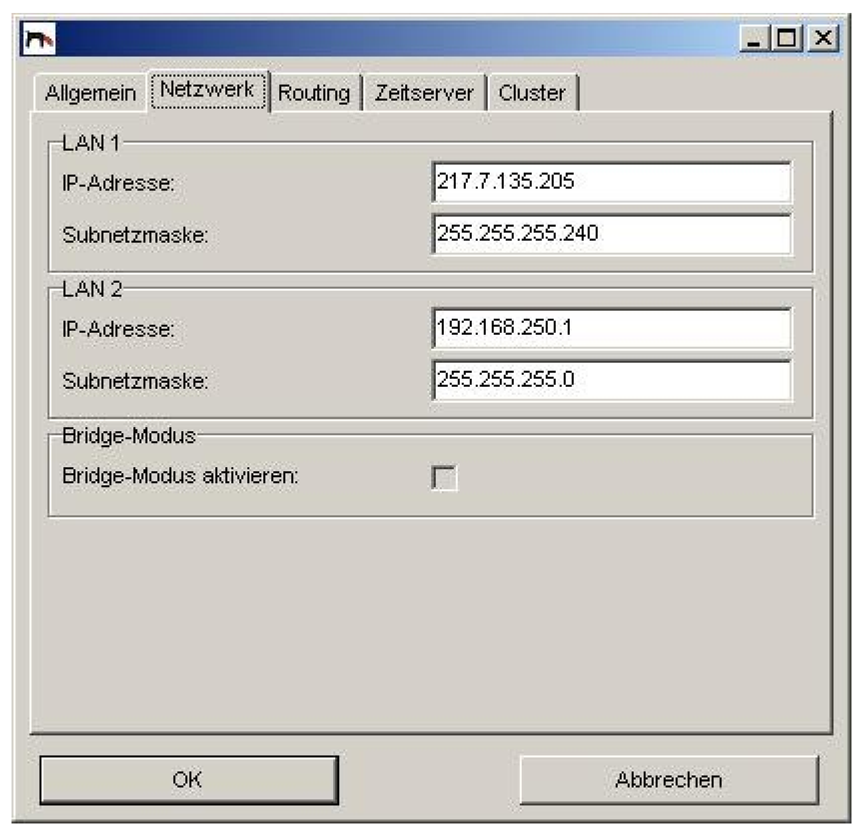



Abbildung: Netzwerk Konfiguration der REDDOXX Appliance

2. *LAN 1 - IP-Adresse:*
   Geben Sie die IP-Adresse der REDDOXX Appliance an.
   Der Standardwert wurde aus den ersten Einstellungen übernommen.
3. *LAN 1 - Netzmaske:*
   Geben Sie die entsprechende Netzmaske der REDDOXX Appliance ein.
   Der Standardwert wurde aus den ersten Einstellungen übernommen.
4. *LAN 2* - ist derzeit deaktiviert. Im Bridge-Mode wird das LAN 2 Interface automatisch konfiguriert.
5. *Bridge-Modus: Bridge-Modus aktivieren:*
   Aktivieren Sie die Checkbox, wenn Sie die Appliance im Bridge-Modus betreiben wollen.
   Eine ausführliche Anleitung zum Bridge-Modus finden Sie in Kapitel 5.
6. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Netzwerk Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Netzwerk Konfiguration.

### 4.2.1.3 Netzwerkeinstellungen - Routing

**Default Gateway und Routing**

Über die Routing Konfiguration können Sie den Default-Gateway einrichten.

**Voraussetzung:** Netzwerk Konfiguration öffnen.

1. Klicken Sie auf den Reiter "Routing".
   Folgende Felder werden angezeigt:

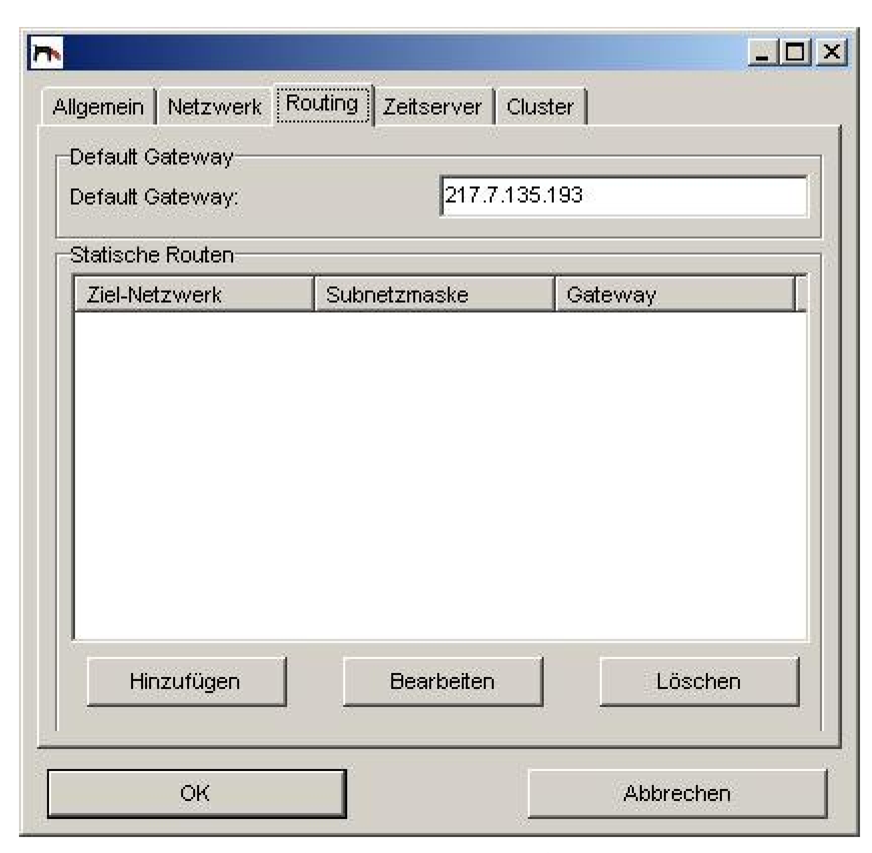



Abbildung: Routing Konfiguration der REDDOXX Appliance

2. *Default-Gateway:*
   Geben Sie hier die IP-Adresse des Default-Gateway ein.
3. Wenn Sie statische Routen hinzufügen wollen, können Sie dies über den Button HINZUFÜGEN machen. Folgende Felder werden angezeigt:

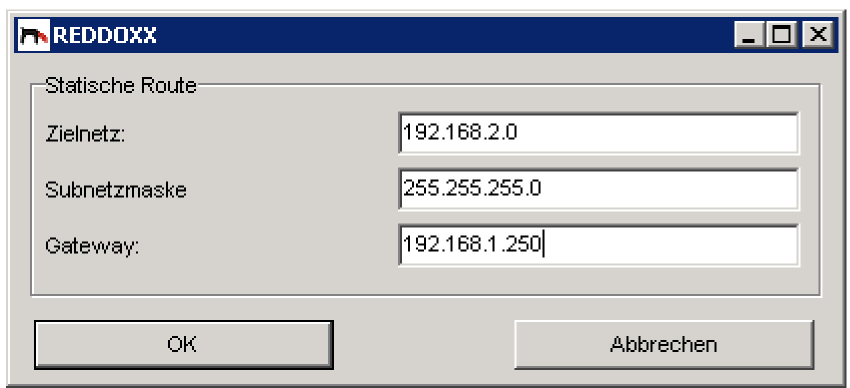



Abbildung: Routing Konfiguration der REDDOXX Appliance

4. Geben Sie einen Zielnetz, die dazugehörige Subnetmaske und ein entsprechendes Gateway ein. Durch klick auf OK wird die Route hinzugefügt.
5. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Netzwerk Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Netzwerk Konfiguration.

### 4.2.1.4 Netzwerkeinstellungen - Zeitserver

**Zeitserver Konfiguration vornehmen**

Über die Zeitserver Konfiguration können Sie die Zeitserver angeben und die zutreffende Zeitzone über die Auswahlliste wählen.

**Voraussetzung:** Netzwerk Konfiguration öffnen.

1. Klicken Sie auf den Reiter "Zeitserver".
   Folgende Felder werden angezeigt:

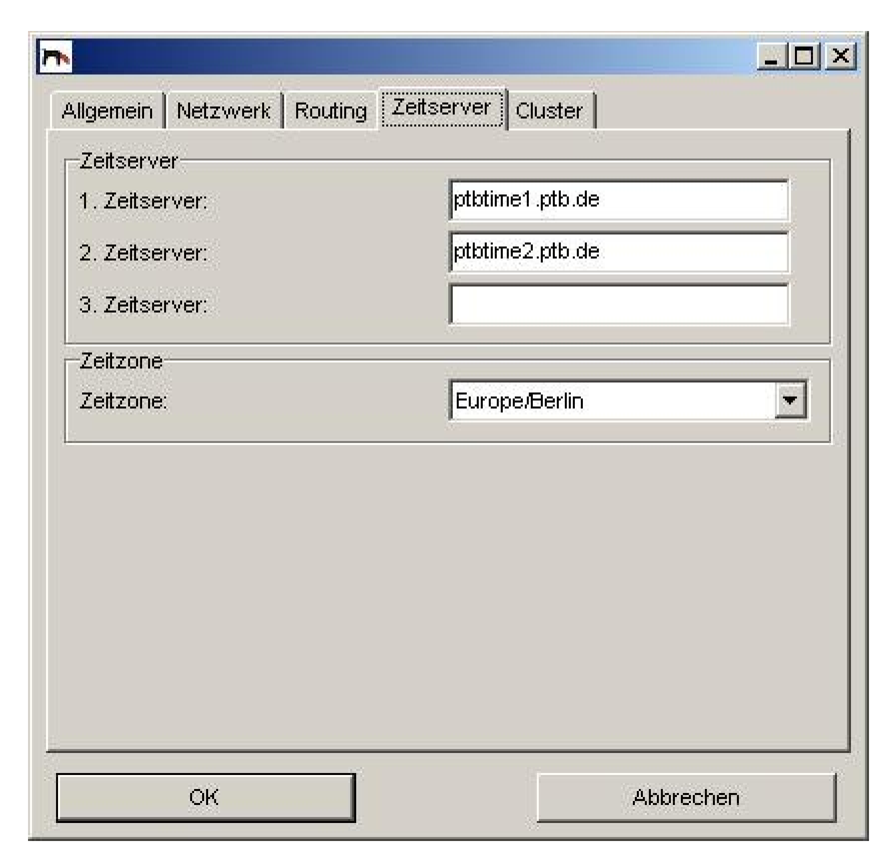


Abbildung: Zeitserver Konfiguration der REDDOXX Appliance

2. *Zeitserver - 1. Zeitserver:*
   Geben Sie den Namen des zu benutzenden Zeitservers an.

**HINWEIS**

Diese Eingabe ist Pflicht! Es wird empfohlen mindestens einen Zeitserver einzutragen, welcher NTP (Network Time Protocol) unterstützt, da die korrekte Zeit für die Funktion der REDDOXX Appliance wichtig ist. Achten Sie darauf, dass der Port 123 UDP an Ihrer Firewall geöffnet ist.

3. *Zeitserver - 2. und 3. Zeitserver:*
   Wiederholen Sie falls notwendig Schritt 2.
4. *Zeitzone - Zeitzone:*
   Wählen Sie über die Auswahlliste die entsprechende Zeitzone aus.
   OK: Speichern und Schließen der Netzwerk Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Netzwerk Konfiguration.

#### 4.2.1.5 Cluster

Laufen Ihre Appliances im Clusterbetrieb, so können Sie die Einstellungen in diesem Reiter kontrollieren. Sie können an dieser Stelle keine Eingaben machen. Änderungen sind ausschließlich über den Cluster Manager in Menü ANSICHT möglich.

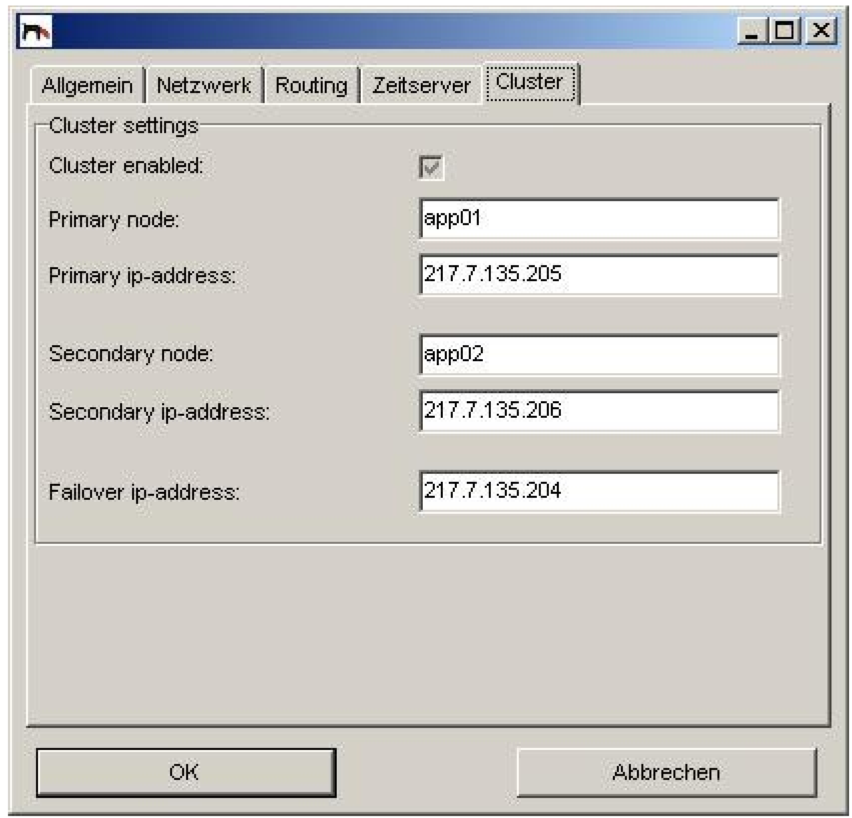



Abbildung: Cluster Einstellungen der REDDOXX Appliance

Cluster enabled: Cluster-Modus aktivieren
Primary node: Bezeichnung der primären Appliance
Primary IP-address: IP-Adresse der primären Appliance
Secondary node: Bezeichnung der sekundären Appliance
Secondary ip-address: IP-Adresse der sekundären Appliance
Failover ip-address: IP Adresse des Clusters.
Klicken Sie auf OK oder auf Abbrechen, um das Fenster zu schließen.

### 4.2.2 Bridge Richtlinien

In der Appliance Konfiguration finden Sie den Punkt Bridge Richtlinien. Hier können Sie Regeln definieren, die bestimmte Teilnehmer (Mail-Clients) oder Internet-Mail-Server vom Proxy-Betrieb ausschließen. Das bedeutet, dass der Internetverkehr für diese Teilnehmer einfach unberücksichtigt und unverändert durchgeschleust wird.

1. Klicken Sie doppelt auf die *Bridge Richtlinien*.
   Folgende Felder werden angezeigt:

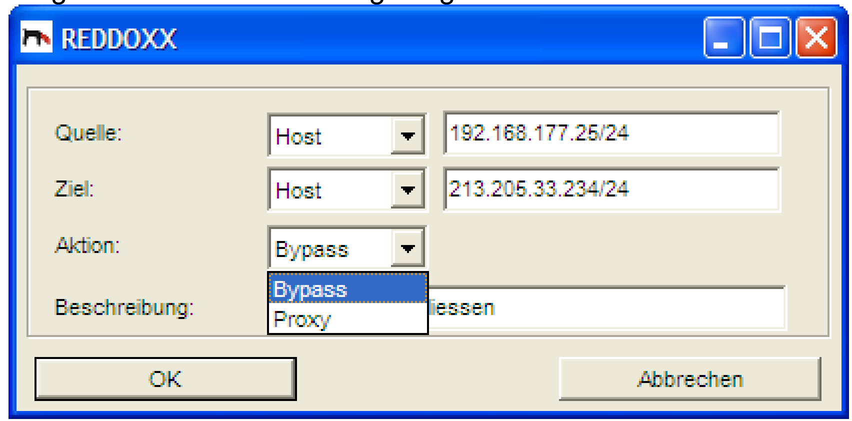



Abbildung: Bridge Richtlinien der REDDOXX Appliance

2. *Quelle*: ist ein Client im internen Netz, alle oder ein bestimmtes Netzwerk
3. *Ziel*: ist der Provider dessen IP Adresse hier eingetragen wird, alle, oder ein bestimmtes Netzwerk
4. *Aktion:*
   „*Bypass*“ - die Mails wird nicht von der Reddoxx, sondern vom Client beim Provider abgeholt.
   „*Proxy*“ – die Mails werden zuerst von der Reddoxx abgeholt, anschließend vom Client.

Sie haben durch die Richtlinien die Möglichkeit verschiedene Regeln zu kombinieren. Die Verarbeitung der Regeln läuft von oben nach unten. Sobald eine Regel zutrifft, wird diese angewendet. Weitere nachfolgende Regeln werden nicht mehr berücksichtigt.

**HINWEIS**

Veränderte Regeln werden erst nach dem Drücken des Aktivieren-Symbols in der Symbolleiste wirksam.

### 4.2.3 Einstellungen

**Einstellungen öffnen**

1. Klicken Sie im Navigationsbaum doppelt auf ***Appliance Konfiguration***.
2. Klicken Sie im Baum den Zweig ***Einstellungen*** doppelt.

#### 4.2.3.1 Einstellungen - Allgemein

**Allgemeine Einstellungen vornehmen**

Über die Allgemeinen Einstellungen können Sie den Hostname und die E-Mail-Adressen der REDDOXX Appliance angeben und verwalten. So kann die REDDOXX Appliance jederzeit an sich oder den Administrator Systemmeldungen senden. Damit die Appliance aktuelle Updates für den Fuzzy-Filter und aktuelle Virenupdates laden kann, muss sie HTTP-Verbindungen ins Internet aufbauen können. Falls dazu ein Proxy Server genutzt werden soll, kann auch dieser hier konfiguriert werden.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Allgemein". Folgende Felder werden angezeigt:

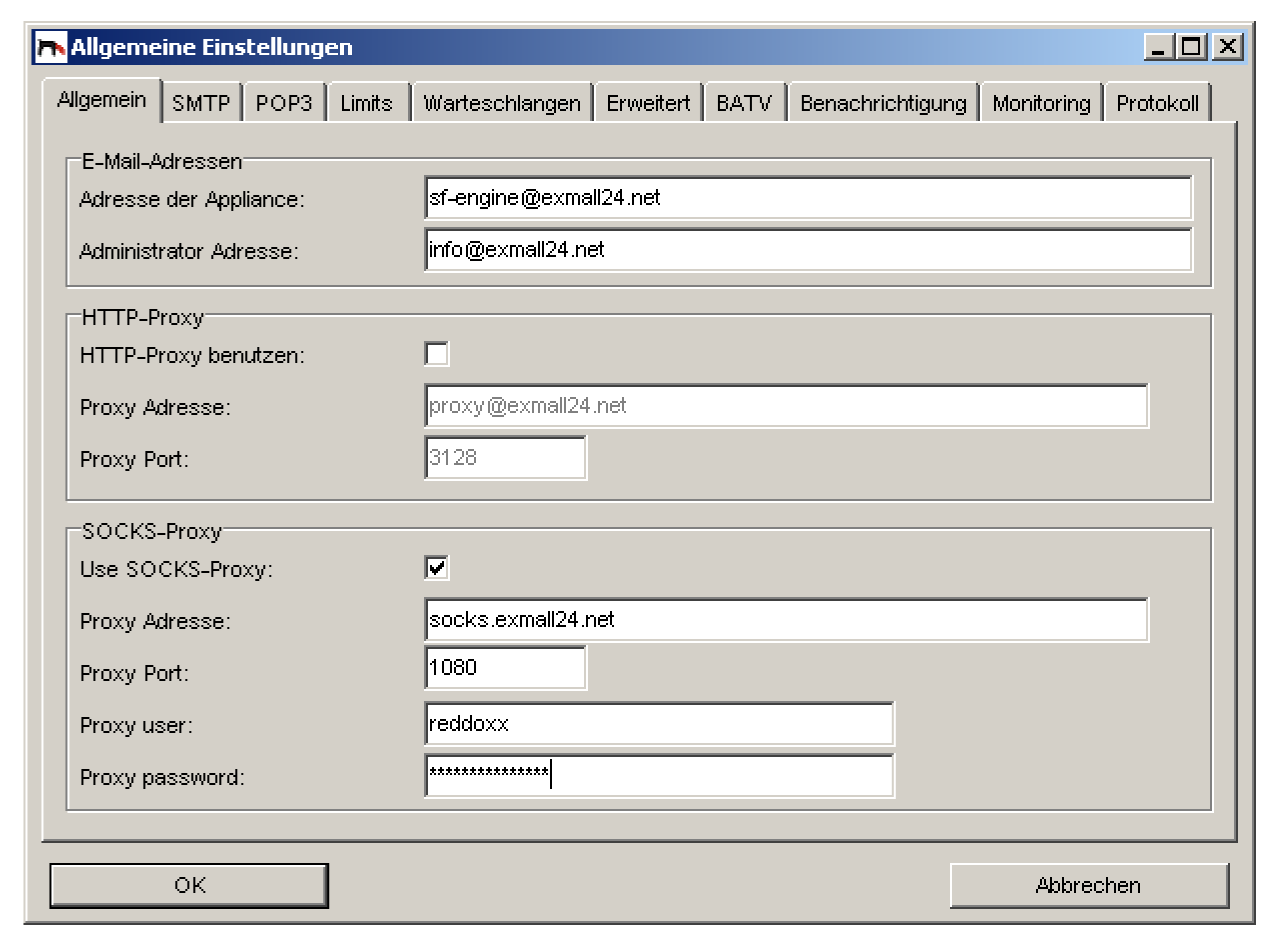



Abbildung: Einstellungen – Allgemein

**E-mail Addressen**

2. *Adresse der Appliance:*
   Geben Sie die E-Mail-Adresse der REDDOXX Appliance an.

   **HINWEIS**

   Die E-Mail-Adresse der REDDOXX Appliance muss eine E-Mail-Adresse einer gültigen E-Mail-Domäne sein und auch von der REDDOXX Appliance empfangen werden. Diese E-Mail-Adresse darf nicht anderweitig verwendet werden.

3. *Administrator-Adresse:*
   Geben Sie die E-Mail-Adresse des Administrators an. An dieser E-Mail-Adresse erhält der Administrator Meldungen von der REDDOXX Appliance, beispielsweise wenn das Backup nicht ordnungsgemäß durchgelaufen ist.

**HTTP-Proxy**

4. *HTTP-Proxy benutzen*:
   Für die Nutzung eines HTTP-Proxy aktivieren Sie die Checkbox.
5. *Proxy Adresse:*
   *Geben Sie den Namen oder die IP Adresse des Proxys ein,* über den die HTTP-Kommunikation ermöglicht wird.
6. *Proxy Port*:
   Geben Sie den Port des Proxy-Servers an
7. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Einstellungen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

***SOCKS-Proxy***

8. Use SOCKS-Proxy:
   Falls Sie über keine direkte Internetverbindung verfügen, können Sie auch einen SOCKS-Proxy angeben. Aktivieren Sie dafür die Checkbox. Ein SOCKS Proxy ist protokollunabhängig und somit flexibler.
9. *Proxy Adresse:*
   Geben Sie den Hostnamen oder die IP-Adresse des Socks-Proxy Servers an, der die Internetverbindung herstellt.
10. *Proxy Port:*
    *Geben Sie den TCP Port des* SOCKS Proxy Servers an.
11. *Proxy User:*
    Geben Sie den Benutzernamen ein, der für die Authentifizierung am SOCKS Proxy Server erforderlich ist.
12. *Proxy Password:*
    Geben Sie das dazugehörende Kennwort ein.

### 4.2.3.2 Einstellungen - SMTP

**SMTP Grundeinstellungen vornehmen**

Über die SMTP Einstellungen können Sie die REDDOXX Appliance in Ihr Netzwerk integrieren.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "SMTP".
   Folgende Felder werden angezeigt:

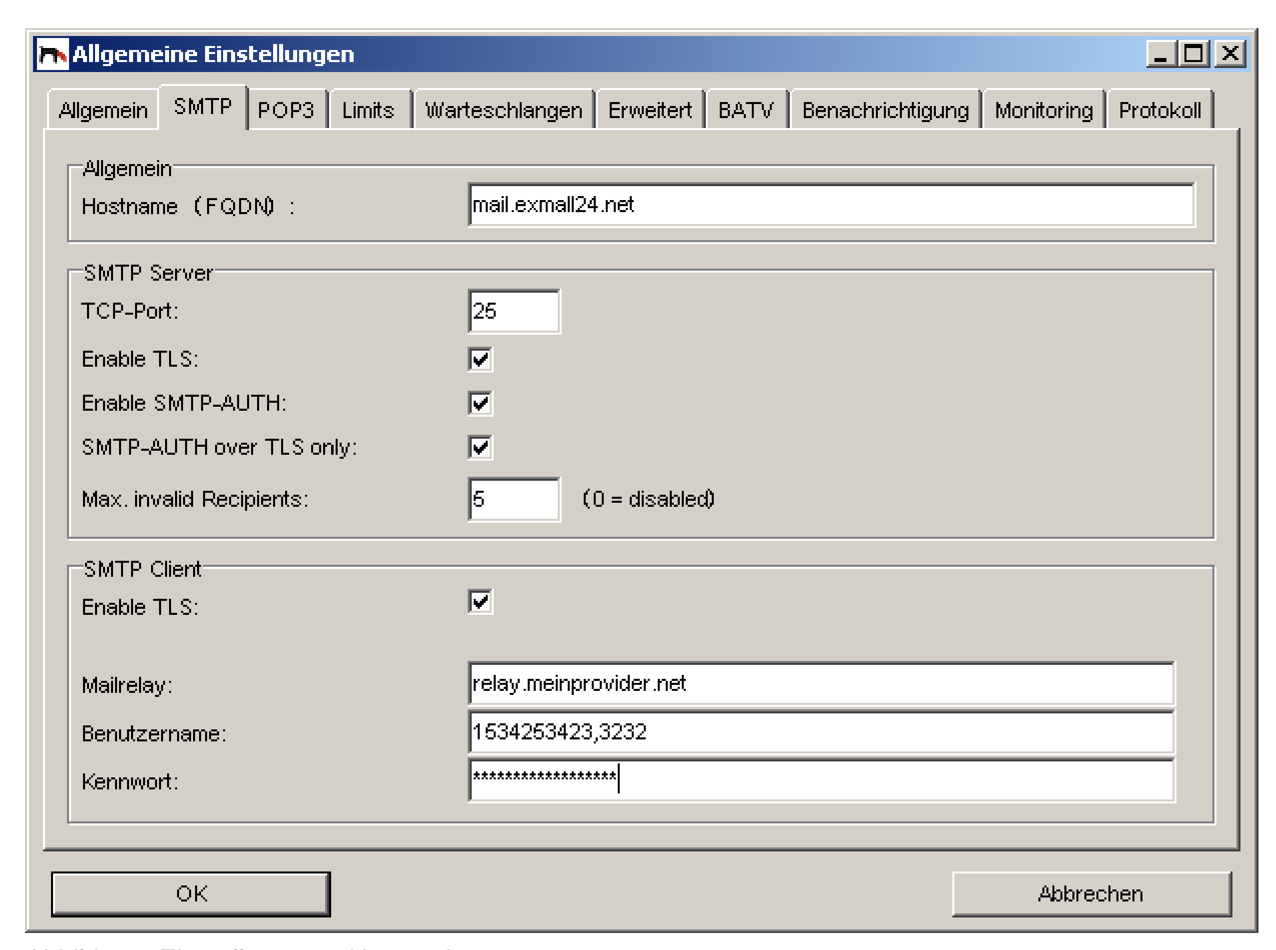



Abbildung: Einstellungen – Netzwerk

## Allgemein

2. *Hostname (FQDN):*
   Geben Sie den entsprechenden Hostname an, mit dem sich die REDDOXX Appliance im Netzwerk identifiziert.
   Dieser Hostname setzt sich aus dem Hostname und der Domäne der Appliance Konfiguration zusammen.

**HINWEIS**

Geben Sie den Hostname im FQDN-Format (Full Qualified Domain Name) ein. Es wird dringend empfohlen, einen Hostnamen zu verwenden, der über eine Reverse-DNS Abfrage (PTR-Eintrag) auflösbar ist, sofern ausgehende Mails NICHT über einen Smarthost (Relay) geleitet werden.

## SMTP-Server

3. *TCP-Port:*
   Passen Sie bei Bedarf den TCP-Port für die SMTP-Verbindungen der REDDOXX Appliance an. Der Standardwert "25" ist vorgegeben.
4. *Enable TLS:*
   Sofern aktiviert, kann die Appliance Eingehende E-Mails verschlüsselt empfangen. Die Appliance erhält bei Beginn einer Transmission den erforderlichen Schlüssel von der Gegenstelle.
5. *Enable SMTP-AUTH*:
   Sofern aktiviert, kann die Appliance über die öffentliche Adresse, also vom Internet aus, E-Mails entgegen nehmen um diese ins Internet zu versenden. Daür muss sich der Versender an der Appliance mit Benutzernamen und Passwort anmelden. Das

bedeutet, dass sich z.B. ein Mitarbeiter in einem externen Büro E-Mails über den allgemeinen Unternehmens-Mail-Server (diese Appliance) versenden kann, ohne dabei per VPN mit dem Unternehmens-Netzwerk verbunden sein muss.

6. *SMTP-Auth over TLS only:*
   Sofern aktiviert, muss der Versender eine verschlüsselte Übertragung mittels TLS wählen, damit er sich an der Appliance anmelden kann, um die „SMTP-Auth“-Funktion nutzen zu können.
7. *Max. invalid Recipients:*
   Die Appliance beendet eine E-Mail-Transmission vorzeitig, wenn die sendende Gegenstelle den Schwellwert für unbekannte (ungültige) Empfänger erreicht hat. Eine “0” deaktiviert diese Funktion. Dies ist der Standardwert.

**NOTICE**

Sie müssen nach Änderungen dieser Einstellungen den SMTP-Server-Dienst neu starten.

**SMTP Client**

8. *Enable TLS*
   Sofern aktiviert, versucht die Appliance die E-Mails mittels TLS verschlüsselt zu übertragen. Falls die Gegenstelle die Verschlüsselung nicht kann, sendet die Appliance unverschlüsselt.
9. *Mail Relay:*
   geben Sie das Mail Relay an, um E-Mails ins Internet zu versenden, falls Sie eins benutzen müssen. E-Mails werden dann nicht direkt zum Empfänger, sondern über das Relay übermittelt. Bevorzugen Sie aber direkte Zustellung, falls dies möglich ist. Dies erfordert eine fest IP-Adresse und einen dazugehörenden PTR-Record im DNS Ihrer Domäne.
10. *Benutzername:*
   Geben Sie den Benutzernamen an, um sich am Mail Relay zu authentifizieren.
11. *Kennwort:*
   Geben Sie zum Benutzernamen das dazugehörende Kennwort an.
12. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   *OK:* Speichern und Schließen der Einstellungen.
   *ABBRECHEN:* Änderungen verwerfen und Schließen der Einstellungen.

**NOTICE**

Benutzernamen und Kennwort müssen nur angegeben werden, sofern eine Anmeldung erfoerdlich ist. Erfragen Sie Benutzernamen und Kennwort von Ihrem Internetprovider.

Sie müssen nach Änderungen dieser Einstellungen den SMTP-Client-Dienst neu starten.

### 4.2.3.3 Einstellungen - POP3

**Pop3 Proxy-Dienste aktivieren**

1. Klicken Sie auf den Reiter "POP3".
   Folgende Felder werden angezeigt:

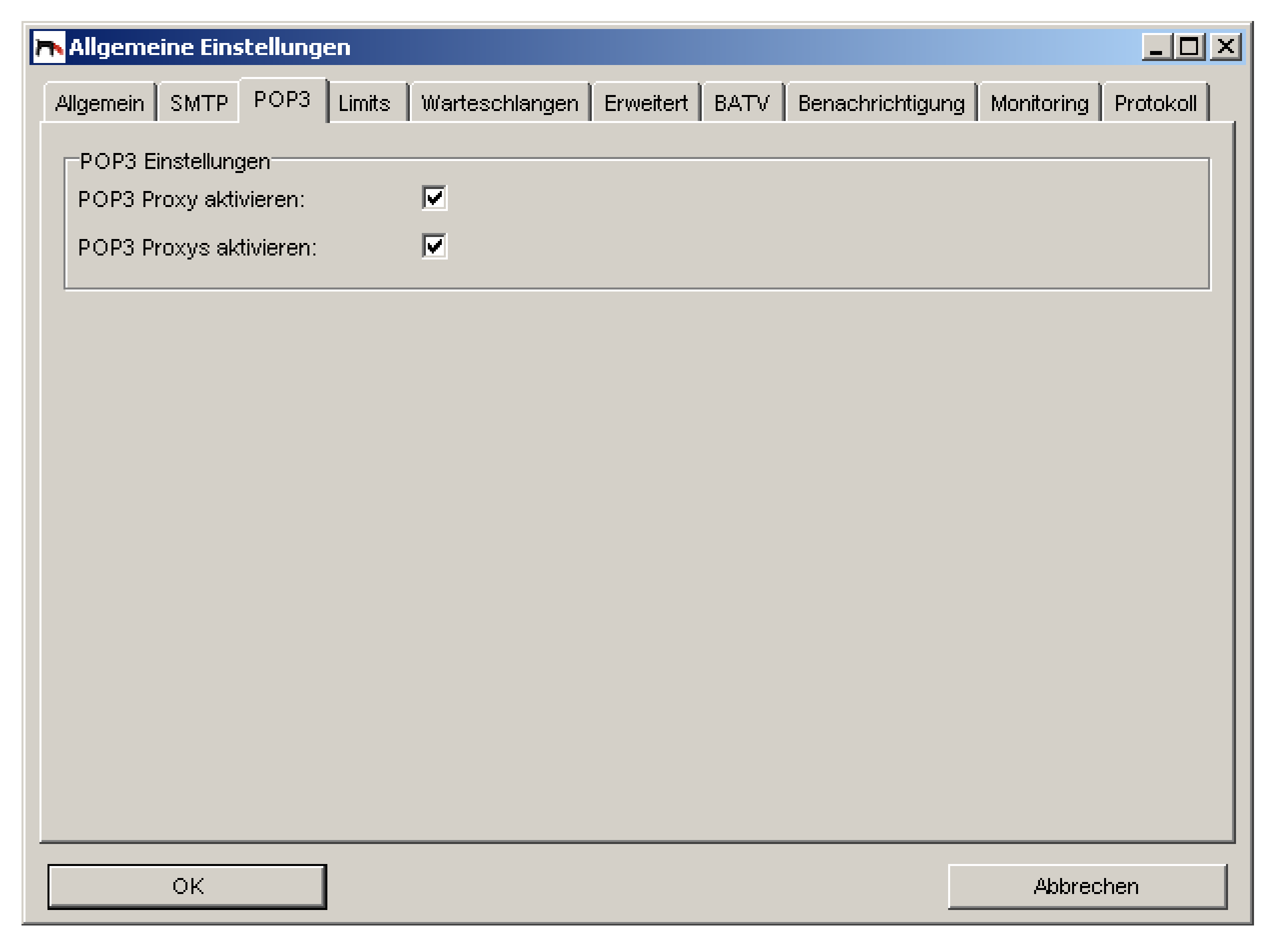



Abbildung: Einstellungen – POP3

**Pop3 Einstellungen**

Weitere detaillierte Informationen zu POP3 und Bridge-Mode finden Sie in der Kurzanleitung unter http://support.reddoxx.net/downloads.php.

2. POP3 Proxy aktivieren
   Aktivieren Sie den POP3 Proxy-Dienst, wenn die REDDOXX Appliance POP3-Anfragen aus dem internen Netz verarbeiten soll. Die Appliance überwacht dabei den TCP-Port 110.
3. POP3 Proxys aktivieren (SSL)
   Aktivieren Sie den Secure POP3 Dienst, wenn die REDDOXX Appliance verschlüsselte POP3-Anfragen aus dem internen Netz verarbeiten soll. Die Appliance überwacht dabei den TCP-Port 995.

### 4.2.3.4 Einstellungen - Limits

**Limit Einstellungen vornehmen**

Über die Limits Einstellungen können Sie die maximalen SMTP-Verbindungen für eingehende und ausgehende E-Mails einstellen. Weitere mögliche Einstellungen sind TimeOuts für Verbindung und

E-Mail-Versand, sowie die maximale E-Mail-Größe. Auch die maximale Anzahl der Konsolen, die sich gleichzeitig zur REDDOXX Appliance verbinden können, kann hier eingestellt werden.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Limits".
   Folgende Felder werden angezeigt:

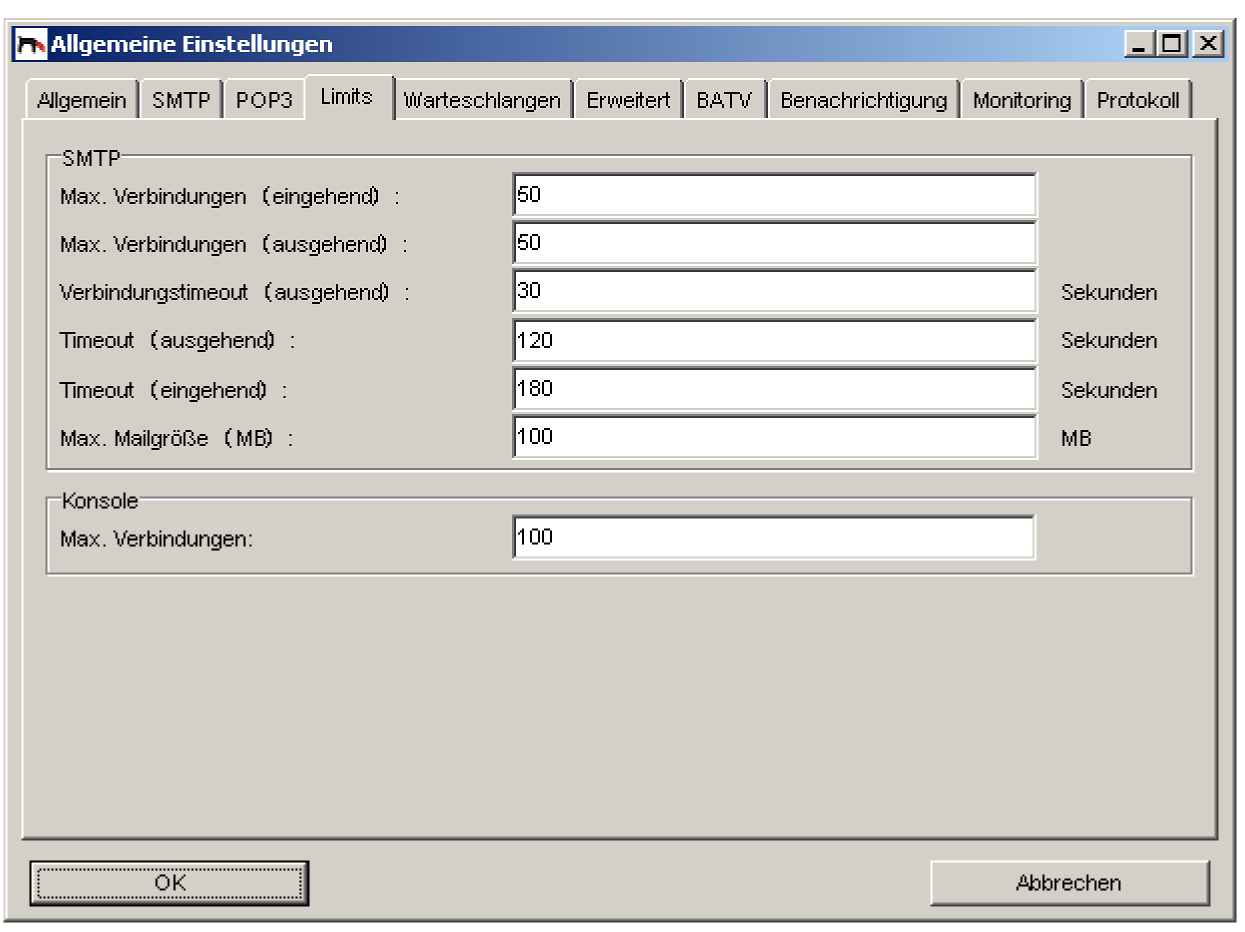



Abbildung: Einstellungen - Limits

**HINWEIS**

Entnehmen Sie für die folgenden Einstellungen die jeweils gültigen Werte aus der Standardwerte-Tabelle, da diese von der erworbenen Variante der REDDOXX Appliance abhängen.

1. *SMTP - Max. Verbindungen (eingehend):*
   Stellen Sie den Grenzwert gleichzeitig eingehender E-Mails ein.
   Dieser Wert definiert, wie viele einkommende SMTP-Verbindungen zur selben Zeit verwaltet und gehalten werden. Verbindungen, die vom internen (lokalen) Netzwerk kommen, haben seit der Version 1024 keine Beschränkung mehr.
2. *SMTP - Max. Verbindungen (ausgehend):*
   Stellen Sie den Grenzwert gleichzeitig ausgehender E-Mails ein.
   Dieser Wert definiert wie viele SMTP-Verbindungen zu anderen Servern zur selben Zeit aufgebaut und gehalten werden.
3. *SMTP - Verbindungstimeout (ausgehend):*
   Stellen Sie den gewünschten Verbindungstimeout für ausgehende E-Mails in Sekunden ein. Diese Zeit definiert, nach wie vielen Sekunden TCP-Kommunikation ohne Antwort, die Verbindung abgebrochen wird.

4. *SMTP - Timeout (ausgehend):*
   Stellen Sie den gewünschten Timeout für ausgehende E-Mails ein. Diese Zeit definiert, nach wie vielen Sekunden ausgehender SMTP- Kommunikation ohne Antwort, die Verbindung abgebrochen wird.
5. *SMTP - Timeout (eingehend):*
   Stellen Sie den gewünschten Timeout für eingehende E-Mails in Sekunden ein. Diese Zeit definiert, nach wie vielen Sekunden eingehender SMTP- Kommunikation ohne Antwort, die Verbindung abgebrochen wird.
6. *SMTP - Max. E-Mail-Größe (MB):*
   Stellen Sie die gewünschte maximale E-Mail-Größe ein. Da während der Datenübertragung eine Prüfung der Größe nicht möglich ist, wird zunächst immer der gesamte Datenteil der E-Mail empfangen und danach geprüft, ob die Grenze überschritten wurde. In diesem Fall erhält die Gegenstelle noch innerhalb des SMTP-Dialoges eine negative Quittung. Die E-Mail wird somit nicht angenommen.
7. *Konsole - Max. Verbindungen:*
   Stellen Sie die maximale Anzahl der Konsolen ein, die sich gleichzeitig zur REDDOXX Appliance verbinden können. Dabei werden sowohl Admin- als auch User-Verbindungen gezählt.
8. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Einstellungen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

**Standardwerte bzw. Empfohlene Einstellungen:**

| | RX-50 | RX-100 | RX-250 | RX-750 | RX-2500 |
|---|---|---|---|---|---|
| Max. Verbindungen (eingehend) | 30 | 100 | 100 | 100 | 200 |
| Max. Verbindungen (ausgehend) | 50 | 150 | 150 | 150 | 200 |
| Verbindungstimeout (ausgehend) | 30 Sek. | 30 Sek. | 30 Sek. | 30 Sek. | 30 Sek. |
| Timeout (ausgehend) | 180 Sek. | 180 Sek. | 180 Sek. | 180 Sek. | 180 Sek. |
| Timeout (eingehend | 180 Sek. | 180 Sek. | 180 Sek. | 180 Sek. | 180 Sek. |
| Max. E-Mail-Größe | 100 MB | 100 MB | 100 MB | 100 MB | 100 MB |
| Max. Konsolen-Verbindungen | 50 | 150 | 150 | 250 | 500 |

**ACHTUNG**

**In der REDDOXX Appliance sind bereits Standardwerte vordefiniert. Diese Standardwerte sollten nicht verändert werden. Ausschließlich Fachpersonal oder der Support dürfen hier Änderungen vornehmen.**

### 4.2.3.5 Einstellungen - Warteschlangen

**REDDOXX Spamfinder Einstellungen über Warteschlangen vornehmen**

Über die Warteschlangen Einstellungen können Sie die Speicherzeiten und Zustellungszeiten der Ausgangswarteschlangen, der CISS Warteschlangen, der Spam Warteschlangen und der Viren Warteschlangen in Tagen festlegen.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Warteschlangen".
   Folgende Felder werden angezeigt:

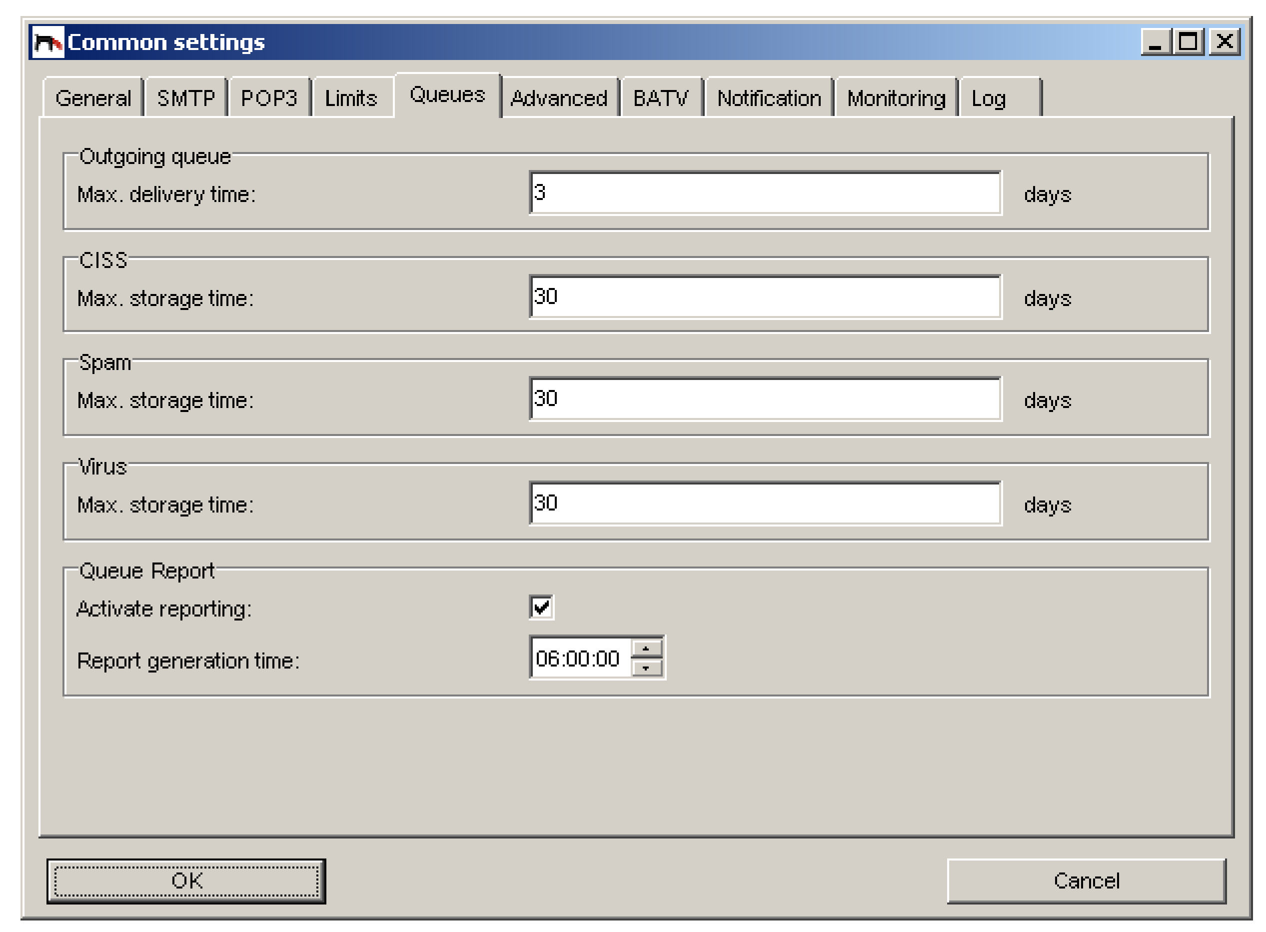



Abbildung: Einstellungen – Warteschlangen

7. *Ausgangswarteschlangen - Max. Zustellungszeit (Tage):*
   Geben Sie die maximale Zustellungszeit der E-Mails der Ausgangswarteschlangen in Tagen an. Während dieses Zeitraums wird versucht, die Mail zuzustellen. Ist der Mailserver, der diese Mails annehmen sollte nach definierter Zeit nicht erreichbar, sendet die REDDOXX dem Absender eine entsprechende Meldung mit SMTP Fehlercode und bricht den Zustellungsprozess ab.
8. *CISS - Max. Speicherzeit (Tage):*
   Geben Sie die maximale Speicherzeit der E-Mails der CISS Warteschlange in Tagen an. Wird eine CISS Aufforderung nach Ablauf der definierten Zeit nicht ausgeführt, so wird die E-Mail auf der Appliance gelöscht und nicht zugestellt.
9. *Spam - Max. Speicherzeit (Tage):*
   Geben Sie die maximale Speicherzeit der E-Mails in der Spam Warteschlange in Tagen an.

Wird bis zum Ablauf der definierten Zeit die Nachricht manuell nicht zugestellt, wird diese gelöscht.

10. *Virus - Max. Speicherzeit (Tage):*
    Geben Sie die maximale Speicherzeit der E-Mails in der Virus Warteschlange in Tagen an.
11. *Warteschlangen Report:*
    Ist dieses Feld aktiviert, wird an jedem Tag zur definierten Berichterstellungszeit für jeden Benutzer dessen Spam- oder CISS-Warteschlange gewachsen ist, ein Warteschlangen Report erstellt. In der User Konsole kann der Benutzer selbst bestimmen ob diese Funktion gewünscht wird und in welchem Format (html/text) diese Benachrichtigung zugestellt werden soll.
12. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
    OK: Speichern und Schließen der Einstellungen
    ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

**HINWEIS**

Bei den angegebenen Standardwerten handelt es sich um unsere Empfehlungen, die aber jederzeit von Ihnen geändert werden können.

Prüfen Sie von Zeit zu Zeit Ihre Einträge und setzen Sie gegebenenfalls die Zeiten runter.

**ACHTUNG**

**Nach Ablauf der eingestellten Zeiten, werden die E-Mails unwiderruflich aus der jeweiligen Warteschlange gelöscht.**
**Hierbei sind die unter "Appliance Konfiguration - Zeitserver" eingestellten Parameter, vor allem die eingestellte Zeitzone, maßgebend.**

### 4.2.3.6 Einstellungen - Erweitert

**Erweiterte Einstellungen vornehmen**

Über die Erweiterten Einstellungen können Sie den E-Mail-Relay, den Validator, Den Standard-Anzeigezeitraum Ihrer Warteschlangen und des Archivs, sowie die Dynamische IP-Blacklist-Funktion einrichten.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Erweitert".
   Folgende Felder werden angezeigt:

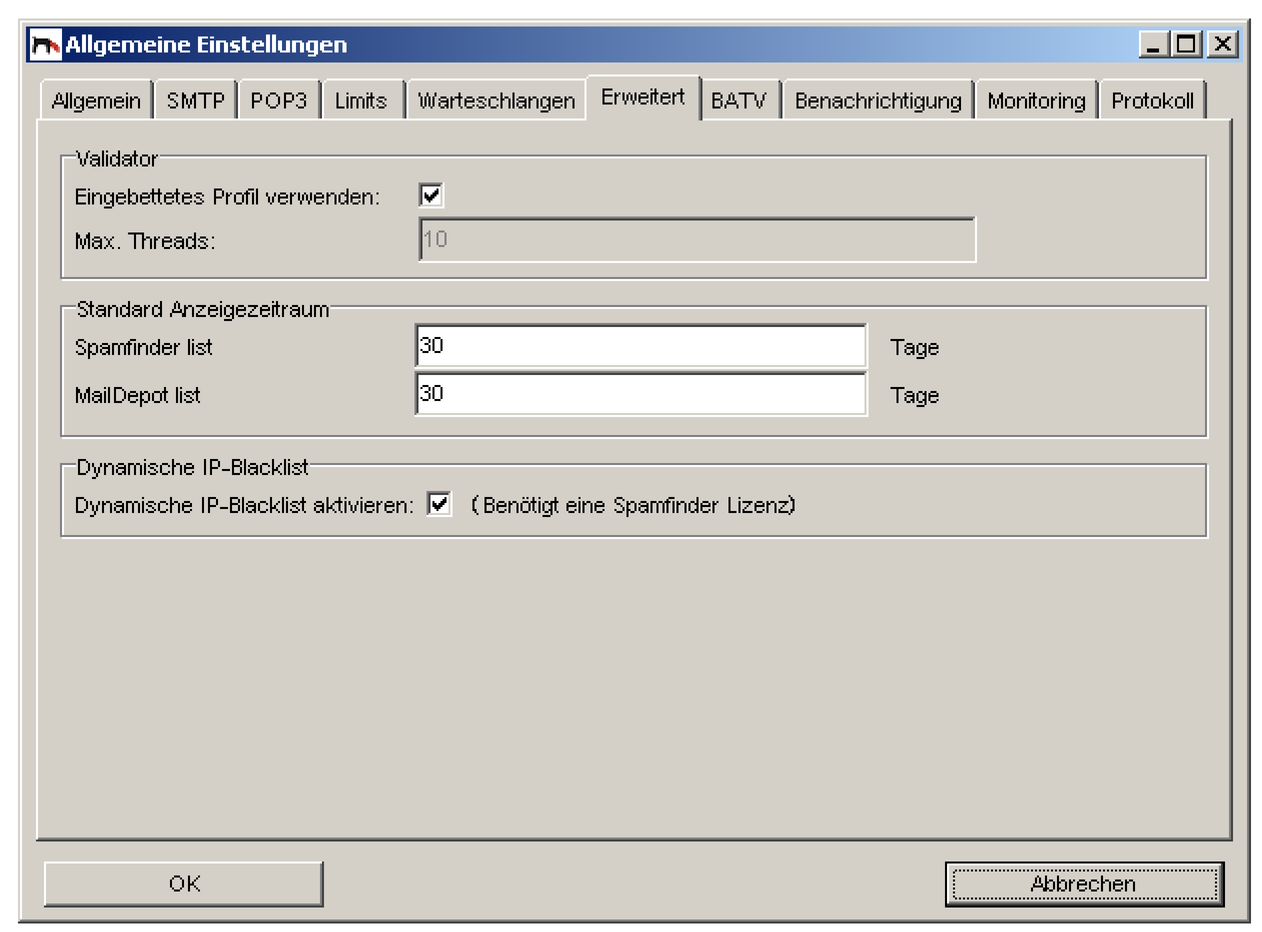



Abbildung: Einstellungen - Erweitert

**Validator**

2. *Eingebettetes Profil verwenden:*
   Ist dieses Feld aktiviert, benutzt die Appliance das *Built-In* Profil, wenn (noch) kein Filterprofil dem E-Mail-Alias zugeordnet ist, oder wenn keine Lizenzen (mehr) vorhanden sind. Weitere Details siehe Kapitel 4.4.2.7.
3. *Max. Threads:*
   Dieser Parameter ist fest vergeben und kann nicht verändert werden. Er bestimmt, wie viele Validierungen parallel verarbeitet werden können.

**Standard Anzeigezeitraum**

4. *Spamfinder Liste:*
   Dieser Wert bestimmt, wie viele Tage die initiale Ansicht zurückgeht. Der Standardwert ist 30. Es werden also alle Einträge der letzten 30 Tage angezeigt.

Geben Sie hier einen kleineren Wert ein, wenn der Aufruf der Listenansicht zu lange dauert. Benutzen Sie die Suche wenn Sie weiter zurück blicken möchten.

5. *MailDepot-Liste:*
   wie bei Punkt 7 beschrieben.

**Dynamische IP-Blacklist**

6. Dynamische IP-Blacklist aktivieren:
   Ist dieses Feld aktiviert, wird bereits beim SMTP-Verbindungsaufbau für den Empfang einer E-Mail geprüft, ob die Sender-IP-Adresse auf einer Blacklist steht. Hierzu werden alle Blacklist-Server verwendet, die in der Filterkonfiguration RBL-Filter angegeben sind. Steht die IP-Adresse auf einer Blacklist, wird der Mailempfang sofort abgebrochen. Vorteil dieser Funktion ist, dass dadurch Ihre Appliance bei massiven Spam-Attacken deutlich weniger belastet wird. Voraussetzung dabei ist, dass E-Mails direkt, also nicht über ein Relay, zugestellt werden. Die Abfragen der RBL-Filter werden zwischengespeichert und sind unter **„gesperrte IP-Adressen“** gelistet. Ein Eintrag ist für einen Tag gültig.

**HINWEIS**

Für die Nutzung der dynamischen IP-Blacklist-Funktion ist eine gültige Spamfinder-Lizenz erforderlich. Erkannte Spam-E-Mails werden nicht in die Spam-Warteschlange gestellt. Ist diese Funktion nicht aktiv, können dennoch die RBL-Filter während des üblichen Validierungsprozesses verwendet werden.

7. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Einstellungen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

### 4.2.3.7 Einstellungen – BATV

**Bounce Address Tag Validation**

Eine weitere Methode Spam zu erzeugen ist die des Bounce Address Spoofings. Dabei wird eine E-Mail mit gefälschtem Absender (z.B. Ihre Adresse) an einen Mail-Server mit unbekanntem Empfänger gesendet. Dieser Mailserver nimmt zunächst die E-Mail an und prüft danach die Zustellbarkeit. Bei Unzustellbarkeit wird an den Sender eine Bounce-Mail zurück gesendet. Da als Absender aber Ihre Adresse angegeben wurde, erhalten Sie die Bounce-Mail, die neben einer einleitenden Fehlermeldung auch den eigentlichen Spam beinhaltet.
Die BATV-Funktion prüft beim Eingang einer Bounce-Mail, ob hierfür zuvor eine E-Mail überhaupt versendet wurde. Falls nicht, wird die E-Mail bereits bei der Zustellung abgelehnt. Sie wird nicht in die Spam-Warteschlange gestellt.

1. Klicken Sie auf den Reiter "BATV".
   Folgende Felder werden angezeigt:

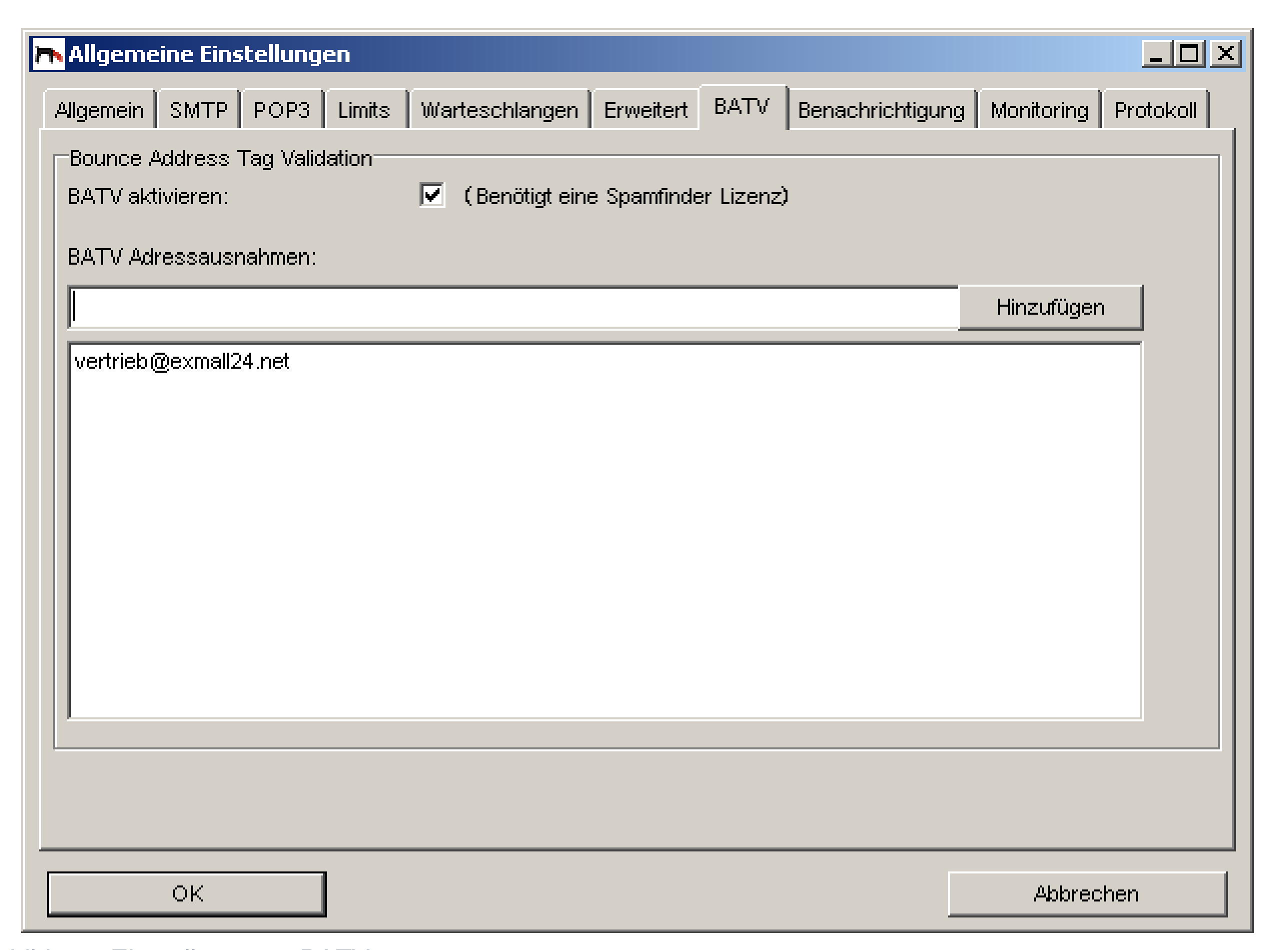



Abbildung: Einstellungen – BATV

2. BOUNCE ADDRESS TAG VALIDATION – BATV aktivieren:
   Aktivieren Sie diese Checkbox, wenn gefälschte Bounce-E-Mails gefiltert werden sollen. Hierfür ist eine gültige Spamfinder-Lizenz erforderlich.
3. BATV ADRESSAUSNAHMEN:
   Falls vereinzelte lokale Empfänger E-Mails, die fälschlicherweise als Bounce-E-Mails gekennzeichnet sind, nicht erhalten sollten, (z.B. Newsletter oder Mails von Shopsystemen ohne regulären Absender) können Sie diese Empfänger aus der BATV-Prüfung herausnehmen. Fügen Sie dazu deren E-Mailadresse in das Feld ein und klicken Sie auf HINZUFÜGEN. Sie können Adressen wieder löschen, indem Sie diese markieren und dann die ENTFernen-Taste drücken.
4. OK: Speichern und Schließen der Einstellungen. Der BATV-Filter wird sofort wirksam.
   ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

**HINWEIS**

Für die Nutzung der BATV-Funktion ist eine gültige Spamfinder-Lizenz erforderlich. Die durch BATV-erkannten Spam-Mails werden nicht in die Spam-Warteschlange gestellt.

Des Weiteren ist es erforderlich, dass Ihre ausgehenden E-Mails auch über die REDDOXX Appliance versendet werden.

### 4.2.3.8 Einstellungen - Benachrichtigung

Sie haben die Möglichkeit Benachrichtigungen der Appliance (z.B. Fehlermeldungen beim Backup oder Fehler, die durch die automatische Diagnose erkannt wurden) direkt an einen SMTP-Server zu senden. Ist nichts eingetragen, wird die Benachrichtigung über die

Appliance versendet. Hat die Appliance aber selbst ein Problem mit dem Versenden einer Mail, wird möglicherweise die Benachrichtigungs-Mail nicht zugestellt.

1. Klicken Sie auf den Reiter "Benachrichtigung".
   Folgende Felder werden angezeigt:

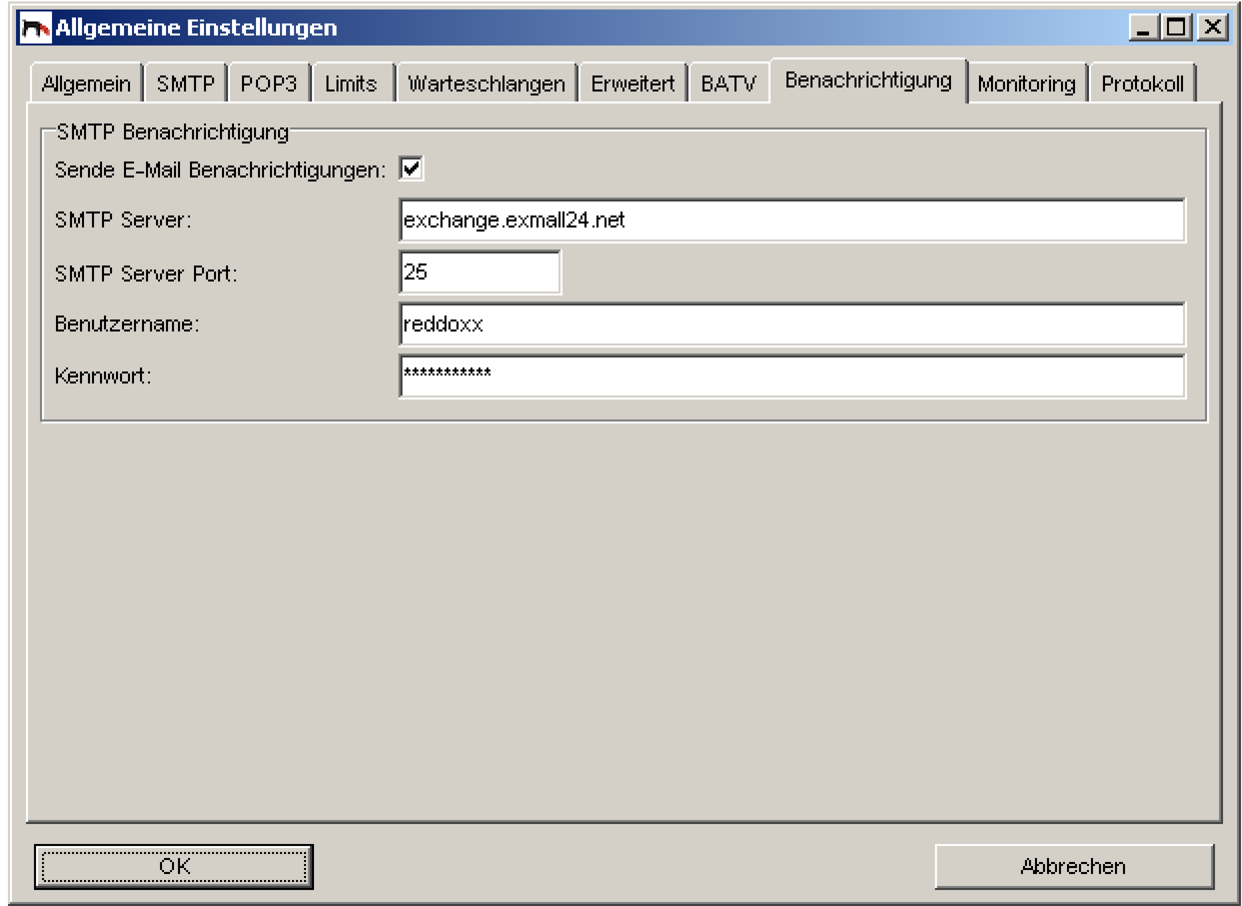



Abbildung: SMTP-Benachrichtigung

**SMTP Benachrichtung**

1. SENDE E-MAIL BENACHRICHTIGUNGEN:
   Setzen Sie den Haken um den Benachrichtungsdienst zu aktivieren. Der Dienst ist standardmäßig aktiviert
2. SMTP SERVER:
   Der Mail Server, über den die Benachrichtigungs-Mail versendet werden soll.
3. SMTP SERVER PORT:
   Der Mail Server TCP-Port, über den der Verbindungsaufbau zum SMTP-Server läuft.
4. BENUTZERNAME
   Der Benutzername, mit dem die Appliance sich beim SMTP-Server autorisiert, um eine Benachrichtigungs-E-Mail versenden zu können.
5. Kennwort:
   Das Kennwort für die Authentifizierung passend zum Benutzername.

**HINWEIS**

Insbesondere beim Betrieb eines Failover Clusters sollte der SMTP Benachrichtigungsdienst aktiviert und ein SMTP-Server angegeben sein, damit Sie beim Ausfall eines Cluster-Knoten per E-Mail informiert werden können.

## 4.2.3.9 Einstellungen - Monitoring

Über das Monitoring können System- und Anwendungswerte der Appliance überwacht werden. Hierfür unterstützt die REDDOXX Appliance das Simple Network Management Protocol (SNMP).
Als Monitoring-Tool kann somit jede Software benutzt werden, die den Umgang mit SNMP beherrscht. So kann der Administrator z.B. die Warteschlangenlänge überwachen, damit beim Überschreiten einer Obergrenze (z.B. 500 E-Mails) das Monitoring System einen Alarm auslöst. Der Administrator kann dann erforderliche Maßnahmen treffen, damit die REDDOXX Appliance die eingehenden E-Mails schneller verarbeiten kann. (Z.B. Hardware-Leistung erhöhen).

### 4.2.3.9.1 SNMP Konfiguration

1. Klicken Sie auf den Reiter "Monitoring".
   Folgende Felder werden angezeigt:

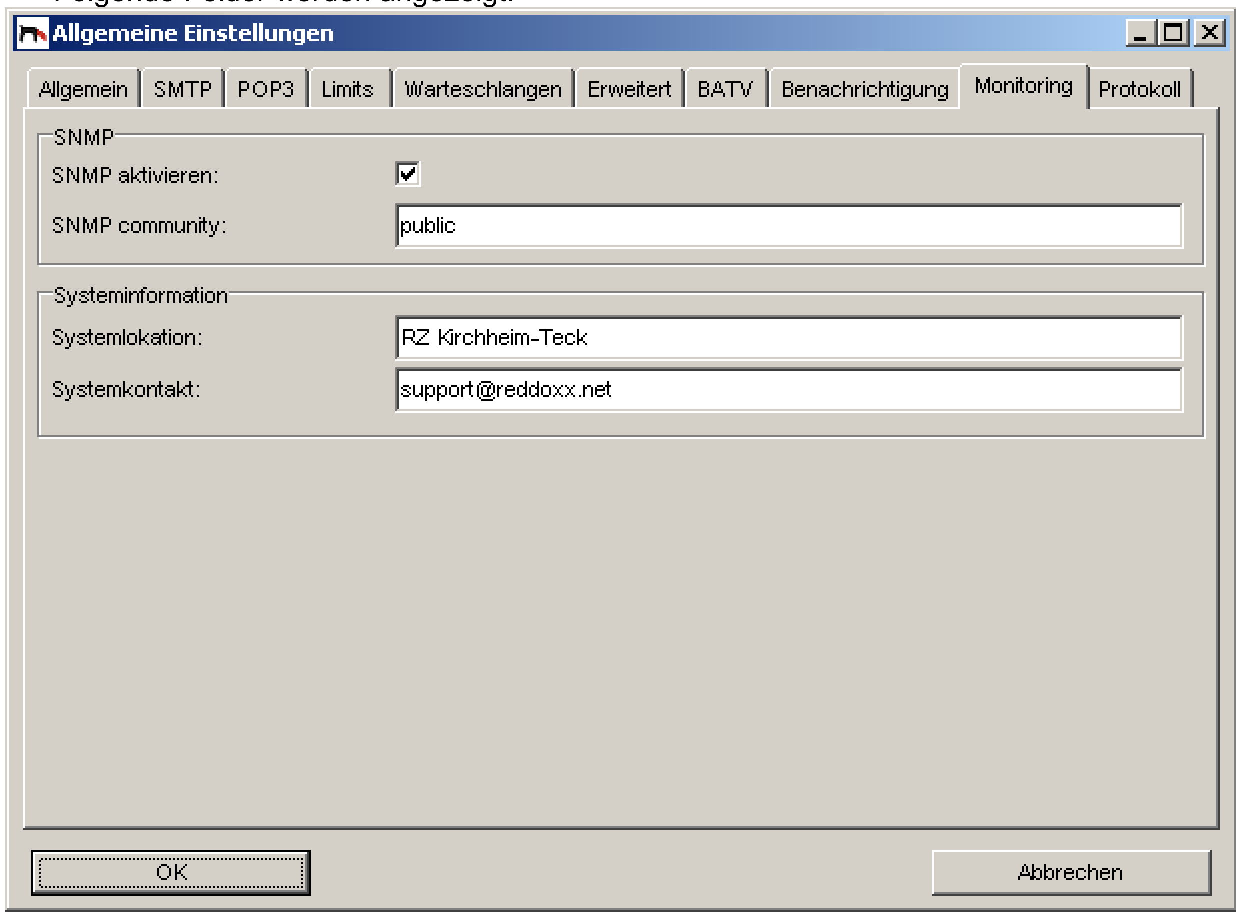



Abbildung: Monitoring mit SNMP

**SNMP**

1. *SNMP aktivieren:*
   Sofern aktiviert, können SNMP-basierende Daten aus der Appliance ausgelesen werden.
2. *SNMP community:*
   Eine Art Kennwort um Zugrif auf die Appliance zu erhalten um SNMP-Daten auslesen zu können.

**Systeminformation**

3. *Systemlokation:*
   Der Standort, wo die Appliance sich befindet.
4. Systemkontakt:
   Eine Adresse des Verantwortlichen dieser Appliance.
5. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Einstellungen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Einstellungen.

### 4.2.3.9.2 SNMP Object IDs

Damit der Systemverwalter des Monitoring Systems auch die Werte der REDDOXX Appliance abfragen kann, benötigt er Object-IDs.
Die Root-Object-ID für REDDOXX lautet 31581. Die einzelnen Messwerte (Keys) werden über die Object-IDs addressiert, wie in nachfolgender Tabelle aufgelistet.

| Object-ID | Key | Description |
|---|---|---|
| enterprises.31581.1.1.1 | rdxSmtpServerConnectionsIn | Reddoxx SMTP Server Inbound Connections |
| enterprises.31581.1.1.2 | rdxSmtpServerConnectionsOut | Reddoxx SMTP Client Outbound Connections |
| enterprises.31581.1.2.1 | rdxSmtpServerMsgRecvIn | Reddoxx Amount of inbound messages received |
| enterprises.31581.1.2.2 | rdxSmtpServerMsgRecvOut | Reddoxx Amount of outbound messages received |
| enterprises.31581.1.3.1 | rdxSmtpServerBytesRecvIn | Reddoxx Amount of bytes received inbound |
| enterprises.31581.1.3.2 | rdxSmtpServerBytesRecvOut | Reddoxx Amount of bytes received outbound |
| enterprises.31581.1.4 | rdxSmtpServerActiveSessions | Reddoxx Number of active SMTP connections |
| enterprises.31581.2.1.1 | rdxSmtpClientConnectionsIn | Reddoxx Amount of inbound SMTP-Client connections |
| enterprises.31581.2.1.2 | rdxSmtpClientConnectionsOut | Reddoxx Amount of outbound SMTP-Client connections |
| enterprises.31581.2.2.1 | rdxSmtpClientMsgSentIn | Reddoxx Amount of inbound messages sent |
| enterprises.31581.2.2.2 | rdxSmtpClientMsgSentOut | Reddoxx Amount of outbound messages sent |
| enterprises.31581.2.3.1 | rdxSmtpClientBytesSentIn | Reddoxx Amount of bytes sent inbound |
| enterprises.31581.2.3.2 | rdxSmtpClientBytesSentOut | Reddoxx Amount of bytes sent outbound |
| enterprises.31581.2.4 | rdxSmtpClientSessions | Reddoxx Current number of outgoing SMTP connections |
| enterprises.31581.2.5 | rdxSmtpClientQueueLength | Reddoxx Messages to be sent |
| enterprises.31581.3.1 | rdxValidatorSessions | Reddoxx Validation Sessions |
| enterprises.31581.3.2 | rdxValidatorQueueLength | Reddoxx Validation Queue Length |
| enterprises.31581.4.1 | rdxArchiveMsgCount | Reddoxx Archived Messages |

| | | |
|---|---|---|
| enterprises.31581.10.1 | rdxSpamfinderRecjects | Reddoxx Rejected Messages |
| enterprises.31581.10.2 | rdxSpamfinderTagMessages | Reddoxx Tagged Messages |
| enterprises.31581.10.3 | rdxSpamfinderCissQuarantine | Reddoxx CISS Quarantined Messages |
| enterprises.31581.10.4 | rdxSpamfinderSpamQuarantine | Reddoxx Quarantined Messages |
| enterprises.31581.10.5 | rdxSpamfinderSpamBounced | Reddoxx Bounced Messages |
| enterprises.31581.10.6 | rdxSpamfinderVirusesDetected | Reddoxx Viruses Detection |
| enterprises.31581.10.100 | rdxSpamfinderBatvHits | Reddoxx BATV Filter Drops |
| enterprises.31581.10.101 | rdxSpamfinderAddedIpBlacklistEntries | Reddoxx IP-Blacklist Entries |
| enterprises.31581.10.102 | rdxSpamfinderRecipientVerificationHits | Reddoxx Rejected Recipient Addresses |

#### 4.2.3.9.3 MIBs und Templates

Reddoxx stellt auf der Download-Seite im Support-Center eine MIB-Datei zum Download bereit. Die MIB-Datei kann in verschiedensten System Monitoring-Systemen importiert werden. Das erspart dem Administrator das aufwändige Erstellen der Messpunkte.
Des Weiteren wird von Reddoxx ein Template für das Network Monitoring System ZABBIX bereitgestellt, da ZABBIX selbst (noch) keine MIBs importieren kann. Die Templates enthalten neben der Deklaration der Messpunkte auch bereits grafische Darstellungskomponenten (graphs)
Die Messpunkte sind mit dem Community-String „*public*“ vorkonfiguriert.

#### 4.2.3.9.4 Demo Monitoring System

Reddoxx bietet außerdem ein Demo-Monitoring System auf Basis von ZABBIX an, das die REDDOXX Demo-Appliance überwacht. Der Zugang erfolgt über das Demo Center, das auch über das Support Center erreichbar ist.

| | |
|---|---|
| REDDOXX Support Center | http://support.reddoxx.net/ |
| REDDOXX Demo Center | http://demo.exmall24.net/ |
| REDDOXX System Monitoring | http://zabbix.reddoxx.net:12080 |

### 4.2.3.10 Einstellungen - Protokoll

Die Protokolldateien werden eine Zeit lang gespeichert. Sie können das Zeitintervall in dieser Option festlegen.

2. Klicken Sie auf den Reiter "Protokoll".
   Folgende Felder werden angezeigt:

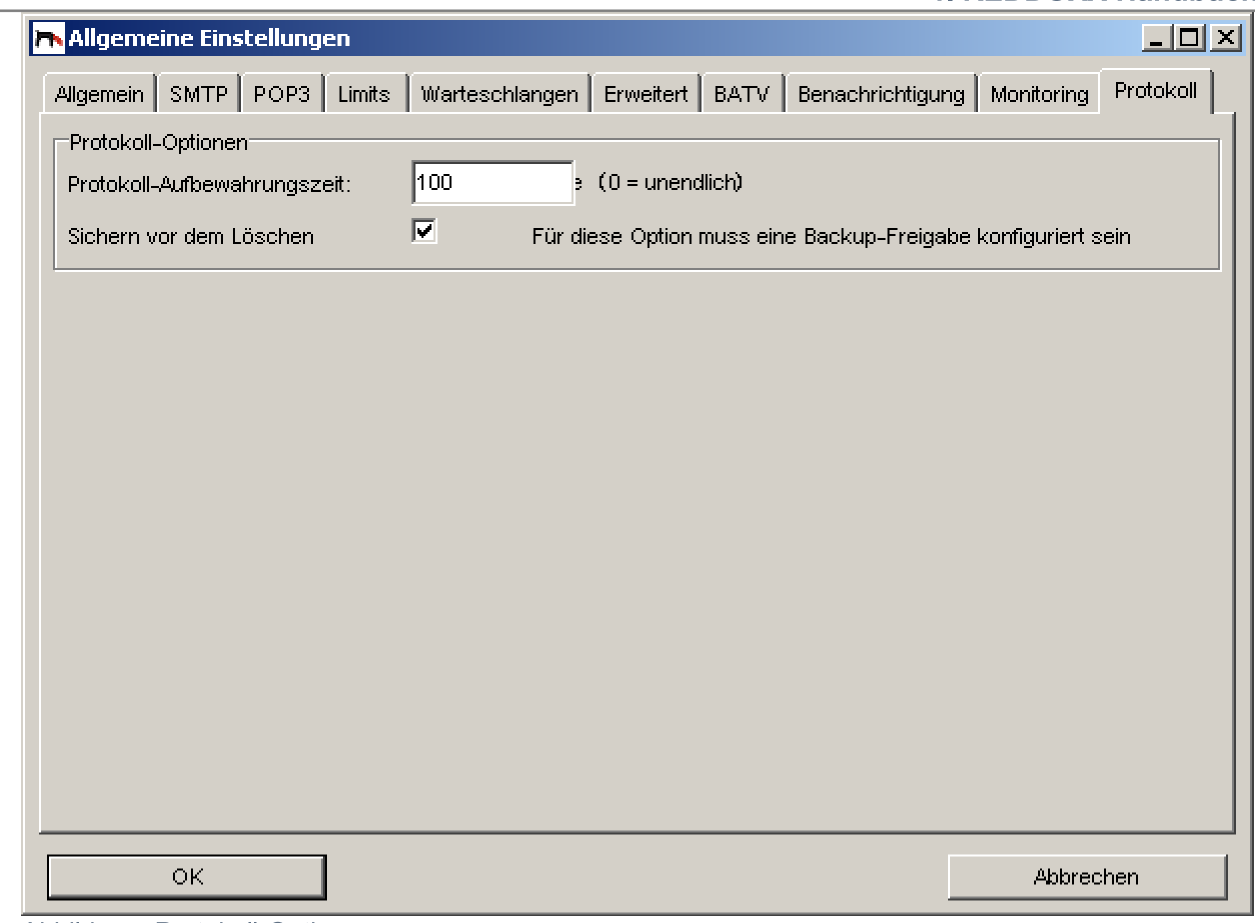


Abbildung: Protokoll-Optionen

3. PROTOKOLL-AUFBEWAHRUNGSZEIT:
   Geben Sie die Zeit (in Tagen) an, in der die Protokolldateien aufbewahrt werden. Nach Ablauf der Zeit werden die älteren Protokolldateien gelöscht.
4. SICHERN VOR DEM LÖSCHEN:
   Mit dieser Option können Sie erzwingen, dass die Protokolldateien nur gelöscht werden, wenn diese zuvor auch gesichert wurden. Als Sicherungs-Ort wird die gleiche Freigabe (Remote Share) benutzt, wie beim Backup.
5. Klicken Sie auf OK um die Einstellungen zu übernehmen.

### 4.2.4 SMTP Konfiguration

#### 4.2.4.1 Lokale Internetdomänen

**Lokale Internetdomänen neu anlegen**

Über die Lokalen Internetdomänen können Sie interne E-Mail-Domänen neu anlegen, für welche die REDDOXX Appliance E-Mails empfangen soll.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Internetdomänen.***
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**.
4. Klicken Sie auf den Reiter "Lokale Internetdomäne".
   Folgende Felder werden angezeigt:

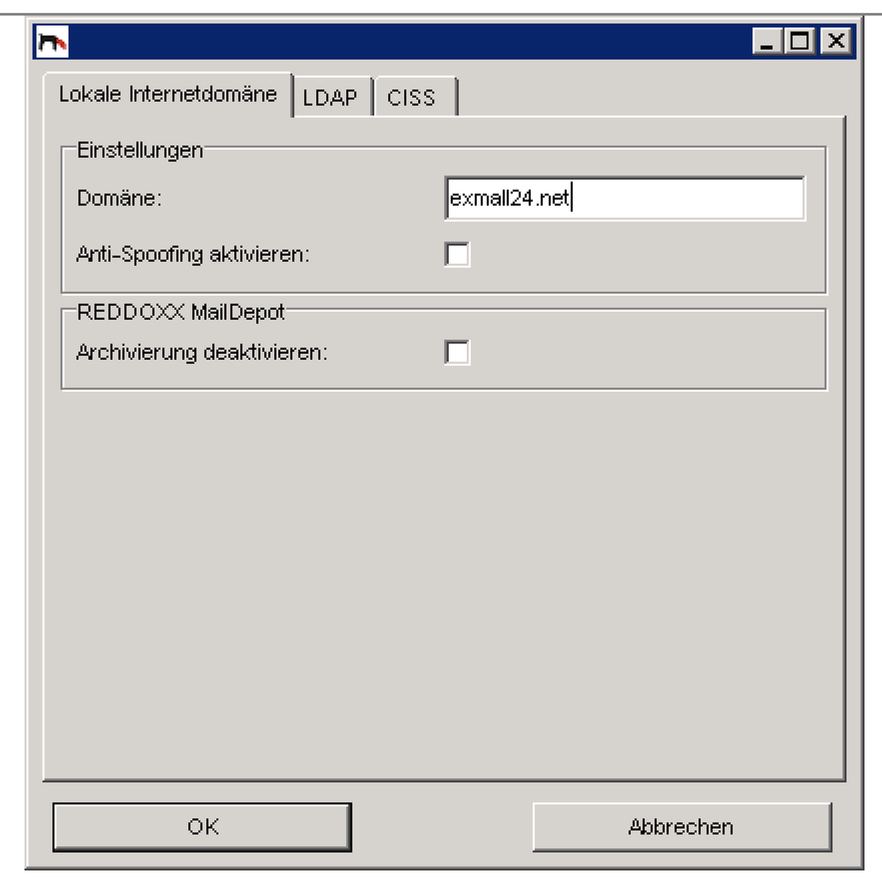



Abbildung: Lokale Internetdomänen

5. *Einstellungen - Domäne:*
   Geben Sie die *Domäne* an, für die Sie E-Mails empfangen möchten.
6. *Einstellungen – Anti-Spoofing aktivieren:*
   Hier können Sie für die jeweilige Domäne das Anti-Spoofing insgesamt aktivieren bzw. deaktivieren.

**HINWEIS**

Um Anti-Spoofing zu aktivieren, muss zusätzlich der Antispoofing-Filter den jeweiligen Filterprofilen zugeordnet werden. Die Funktionsweise und das Bearbeiten von Filtern sind im Kapitel *Filterprofile* beschrieben.

7. *REDDOXX Mail Depot – Archivierung deaktivieren:*
   Ist dieses Feld gesetzt, werden keine E-Mails im MailDepot archiviert.
8. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter: LDAP.
   OK: Speichern und Schließen der Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### LDAP-Einstellungen

Einer der wesentlichen Bestandteile der REDDOXX-Filtertechnik ist die Empfängerprüfung (RVC = Recipient Verify Check). Hier können Sie einstellen, ob E-Mails nur an existierenden Empfängeradressen zugestellt oder abgelehnt werden.
Als Authentifizierungsmethode können Sie zwischen einem unternehmensweiten Verzeichnisdienst und der lokalen Benutzerdatenbank der REDDOXX-Appliance wählen.
**Voraussetzungen:** Lokale Internetdomänen auswählen und Doppelklick auf die zu konfigurierende Domäne.

1. Klicken Sie auf den Reiter "LDAP".
   Folgende Felder werden angezeigt:

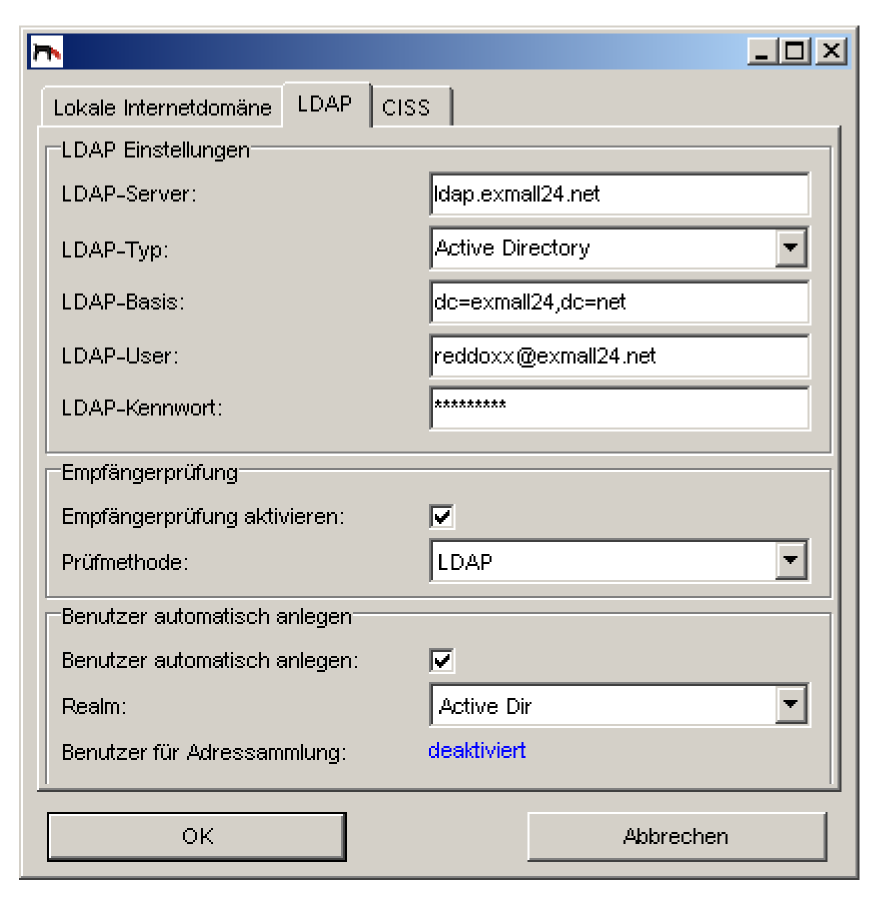



Abbildung: Lokale Internetdomänen – LDAP

## LDAP-Einstellungen

2. *LDAP Server:*
   Geben Sie die IP-Adresse des LDAP-Server an.

**HINWEIS**

Sie können zusätzlich zur IP-Adresse auch einen Port mit angeben, durch Doppelpunkt getrennt (Beispiel: 192.168.0.3:3268). Sofern der LDAP-Server auch über einen GLOBAL CATALOG-Server verfügt (z.B. Microsoft Domain Controller), empfehlen wir diesen bevorzugt anzugeben, da er bis zu 10 x schneller antwortet. Der Default für den Global Catalog ist TCP-Port 3268.

3. *LDAP-Typ:*
   Geben Sie den LDAP-Typ an. Zur Auswahl stehen Active Directory, Exchange 5.5, Lotus Notes Domino und OpenLDAP.
4. *LDAP-Basis:*
   Geben Sie die LDAP-Basis an. Beispiel: dc=company, dc=com
5. *LDAP-User:*
   Geben Sie den User für die Authentifizierung am LDAP-Server an. Sie müssen dabei den vollen UPN-Namen benutzen.
6. *LDAP-Kennwort:*
   Geben Sie das Kennwort für die Authentifizierung am LDAP-Server an.

## Empfängerprüfung

7. *Empfängerprüfung aktivieren:*
   Ist dieses Feld aktiviert, werden E-Mailadressen anhand der konfigurierten LDAP-Schnittstelle, oder der lokal eingetragenen E-Mailadressen geprüft. Dadurch nimmt die REDDOXX Appliance ausschließlich E-Mails an, welche im entsprechenden Verzeichnis (Active Directory, Lotus Domino, etc.), oder lokal gelistet sind.

**HINWEIS**

Nachdem die Empfängerprüfung aktiviert wurde, muss auf der REDDOXX Appliance der Dienst "SMTP Server" neu gestartet werden. Sie finden den Dienst im Verzeichnisbaum unter Appliance Administration.

Weitere Informationen zur LDAP-Konfiguration können Sie im REDDOXX Support Center unter http://support.reddoxx.net  Im Bereich *„Handbücher".*

8. *Prüfmethode:*
   Sie können entweder *LDAP* oder *LOCAL* als Prüfmethode auswählen.

## Benutzer automatisch anlegen

9. *Benutzer automatisch anlegen:*
   Ist dieses Feld aktiviert, werden Benutzer automatisch beim ersten Eintreffen einer E-Mail ein-gerichtet. Dabei wird zuerst geprüft, ob für die E-Mailadresse des Empfängers ein Benutzer im LDAP existiert. Sofern dieser Benutzer im LDAP existiert, wird dieser mit allen zugewiesenen E-Mailadressen auf der Appliance automatisch angelegt. Jeder E-Mailadresse wird dabei automatisch das Default-Filterprofil zugewiesen.
10. *Benutzer automatisch anlegen - Realm:*
    Wählen Sie den Realm, der für die Benutzerüberprüfung verwendet werden soll. Den Realm definieren Sie in der Benutzerverwaltung unter Anmeldekonfiguration.
11. *Benutzer für Adressammlung:*
    Klicken Sie auf das blaue Feld „*deaktiviert*" Es erscheint folgender Dialog:

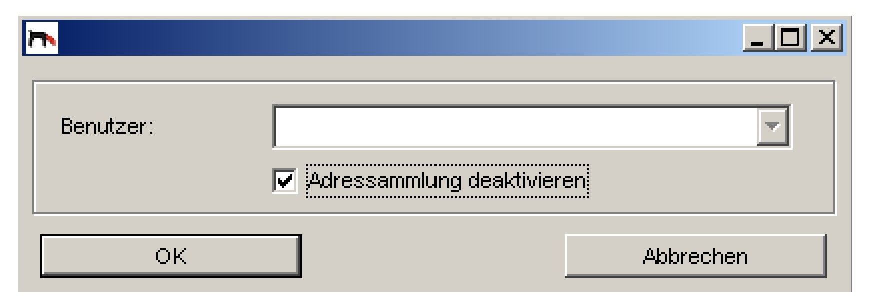



Abbildung: Lokale Internetdomänen – Benutzer für Adressammlung

12. *Adressammlung deaktivieren:*
    Entfernen Sie den Haken in diesem Feld. Dadurch wird die Auswahlbox „Benutzer" freigegeben.
13. *Benutzer:*
    Wählen Sie einen Benutzer aus der Liste aus, dem Sie alle bisher nicht zugeordneten E-Mail-Aliase zuordnen wollen. Dies ist insbesondere für öffentliche Ordner und E-Mail-Verteileradressen hilfreich, für die kein Benutzer aus dem LDAP automatisch zuordenbar ist. Kommen nun E-Mails an eine Verteileradresse an, wird der E-Mail-Alias diesem Benutzer zugeordnet. Dabei wird dem E-Mail-Alias das Default-Filterprofil zugeordnet,

sodass die Spam-Filterung durchlaufen wird. Der ausgewählte Benutzer kann nun diese E-Mails in seinen Warteschlangen verwalten.

14. OK: Speichern und Schließen der Konfiguration.
    ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration

**CISS-Signatur**

Diese optionale Signatur wird an die automatische E-Mail gehängt, die die REDDOXX Appliance zur Benachrichtigung versendet. Die Signatur muss für jede Domäne separat eingegeben werden

**Voraussetzungen:** Lokale Internetdomänen auswählen und Doppelklick auf die zu konfigurierende Domäne.

1. Klicken Sie auf den Reiter "CISS".
   Folgende Felder werden angezeigt:

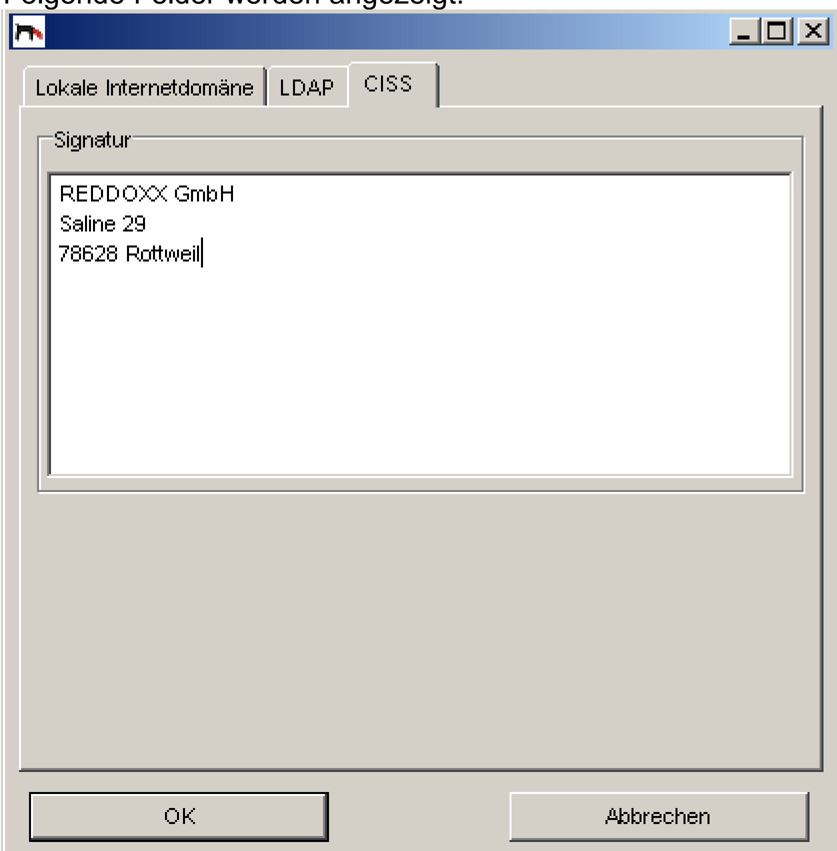



Abbildung: Lokale Internetdomänen - CISS

2. Geben Sie eine beliebige domänenspezifische *Signatur* ein.
   Diese optionale Signatur wird an den Benachrichtigungstext angehängt, den die REDDOXX Appliance bei einer CISS Challenge an den Absender versendet. Sie kann für jede Domäne separat eingegeben werden.

**HINWEIS**

**Siehe auch:** Entnehmen Sie weitere Informationen zum Thema automatisch generierte E-Mail, bitte dem Kapitel "Benachrichtigungen".

3. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### Lokale Internetdomänen bearbeiten

Um eine bereits bestehende Internetdomäne zu bearbeiten, gehen Sie wie folgt vor.
**Voraussetzungen:** Internetdomäne in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Internetdomänen*** aus.
2. Klicken Sie die zu bearbeitende Internetdomäne doppelt an.
   Das Fenster für die Konfiguration öffnet sich.
3. Nehmen Sie alle gewünschten Änderungen vor.
4. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### Lokale Internetdomänen löschen

Um eine bereits bestehende Internetdomäne zu löschen, gehen Sie wie folgt vor.
**Voraussetzungen:** Internetdomäne in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Internetdomänen*** aus.
2. Klicken Sie den zu löschenden Listeneintrag mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit JA, um die Internetdomäne zu löschen.
   NEIN: Internetdomäne wird nicht gelöscht.

*** HINWEIS - INFORMATIONEN ZUR EMPFÄNGERPRÜFUNG**

Durch die Empfängerprüfung versucht die REDDOXX Appliance bereits vor der Nachrichtenübermittlung festzustellen, ob der Empfänger der Nachricht vom internen E-Mail-Server bedient wird.

**Zurzeit werden für diese Funktionen folgende E-Mail-Systeme unterstützt:**

Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Lotus Notes Domino Server

**Konfiguration:**

| BACKEND-TYP | EXCHANGE 5.5 | EXCHANGE 2000 UND 2003 | LOTUS NOTES | OPENLDAP |
|---|---|---|---|---|
| Prüf-Methode | LDAP | LDAP | LDAP | LDAP |
| LDAP-Server | IP/Hostname des Exchange Servers | IP/Hostname eines Domänen-Controllers | IP/Hostname eines Domänen-Controllers | IP/Hostname eines Domänen-Controllers |
| LDAP-Typ | Exchange 5.5 | Active Directory | Lotus Domino | OpenLDAP |
| LDAP-Basis | | dc=company, dc=com (Beispiel) | | dc=company,dc=com (Beispiel) |
| LDAP-User | | UPN des LDAP-Users | | |

| | | | | |
|---|---|---|---|---|
| LDAP-Passwort | | Passwort des LDAP-Users | | |

UPN = User Principal Name
Z.B. ldap-proxy@company.com
Der User wird für die Active Directory oder Lotus Domino Abfrage benutzt und muss die Rechte besitzen, die Eigenschaften der E-Mail-Adresse zu lesen.

**WICHTIG**

**Exchange 5.5**
**Hier wird weder Basis noch Benutzer angegeben (Anonyme Anmeldung).**
**E-Mail-Adressen müssen im Adressbuch veröffentlicht sein!**

### 4.2.4.2 Lokale Netzwerke

**Lokale Netzwerke neu anlegen**

Über die lokalen Netzwerke bestimmen Sie, - von welchen Hosts - oder aus welchen Netzwerken – E-Mails über die REDDOXX versendet werden dürfen.

**Voraussetzungen:** Anmelden an der Administrator-Konsole der REDDOXX.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Netzwerke*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

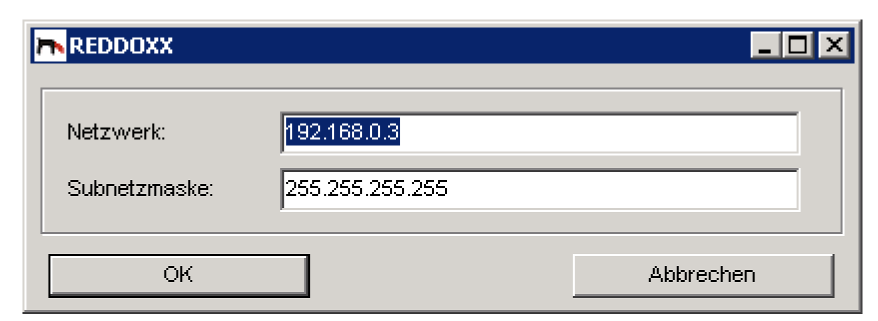



Abbildung: Lokale Netzwerke - Lokales Netzwerk

4. Geben Sie das lokale *Netzwerk* oder einen einzelnen Host ein.
5. Einzelne Hosts, wie z.B. der interne Mailserver benötigen als Maske 255.255.255.255.
6. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**HINWEIS**

Steht vor Ihrer REDDOXX-Appliance ein Mail Relay oder eine Firewall mit einem SMTP-Serverdienst oder einem POP3-Collector Service, der zuerst die E-Mails annimmt, darf diese NICHT in den lokalen Netzwerken stehen.

### Lokale Netzwerke bearbeiten

Um bereits bestehende Netze zu bearbeiten, gehen Sie wie folgt vor.

**Voraussetzungen:** Es sind Einträge in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Netzwerke*** aus.
2. Klicken Sie das zu bearbeitende Netz doppelt an.
   Das Fenster für die Konfiguration öffnet sich.
3. Nehmen Sie alle gewünschten Änderungen vor.
4. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### Lokale Netzwerke löschen

Um eine bereits bestehende Netze zu löschen, gehen Sie wie folgt vor.

**Voraussetzungen:** Netze in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - Lokale Netzwerke*** aus.
2. Klicken Sie den zu löschenden Listeneintrag mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit JA, um die E-Mail zu löschen.
   NEIN: E-Mail wird nicht gelöscht.

**HINWEIS**

Änderungen an den lokalen Netzwerken benötigen einen Neustart des SMTP-Server-Dienstes. Der Neustart eines Dienstes ist in diesem Dokument unter Appliance Administration/Dienste beschrieben.

## 4.2.4.3 E-Mail-Transport

### E-Mail-Transport neu anlegen

Über den E-Mail-Transport können Sie festlegen, an welchen E-Mail-Server die E-Mails der eingetragenen Domäne weitergeleitet werden sollen.

**Voraussetzungen:** Anmelden an der Administrator-Konsole der REDDOXX.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - E-Mail-Transport*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

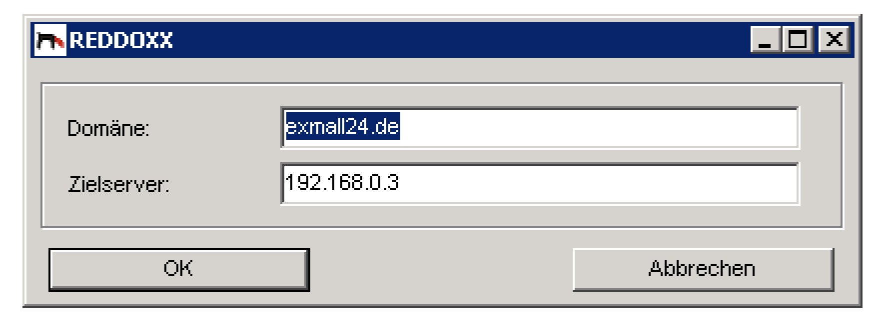



Abbildung: E-Mail-Transport

4. Geben Sie die gewünschte *Domäne* an.
5. Geben Sie den zugehörigen *Zielserver* an.
6. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**HINWEIS**

Wenn die Domäne einer E-Mail hier nicht eingetragen ist, wird der Zielserver über einen DNS-Lookup, auf den in der Konfiguration eingetragenen DNS-Server, ermittelt.

#### E-Mail-Transport bearbeiten

Um bereits bestehende E-Mail-Transporte zu bearbeiten, gehen Sie wie folgt vor.
**Voraussetzungen:** E-Mail-Transport in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - E-Mail-Transport*** aus.
2. Klicken Sie den zu bearbeitenden E-Mail-Transport doppelt an.
   Das Fenster für die Konfiguration öffnet sich.
3. Nehmen Sie alle gewünschten Änderungen vor.
4. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

#### E-Mail-Transport löschen

Um eine bereits bestehende Netze zu löschen, gehen Sie wie folgt vor.
**Voraussetzungen:** E-Mail-Transporte in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration - E-Mail-Transpor***t aus.
2. Klicken Sie den zu löschenden Listeneintrag mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit JA, um die E-Mail zu löschen.
   NEIN: E-Mail wird nicht gelöscht.

### 4.2.4.4 Zugelassene IP-Adressen

Ist ein sendender Mailserver auf einer Blacklist, von dem Sie aber dennoch Mails empfangen können möchten, tragen Sie hier seine IP-Adresse ein.

#### Zugelassene IP Adresse neu anlegen

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration – zugelassene IP-Adressen*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**
   Folgende Felder werden angezeigt:

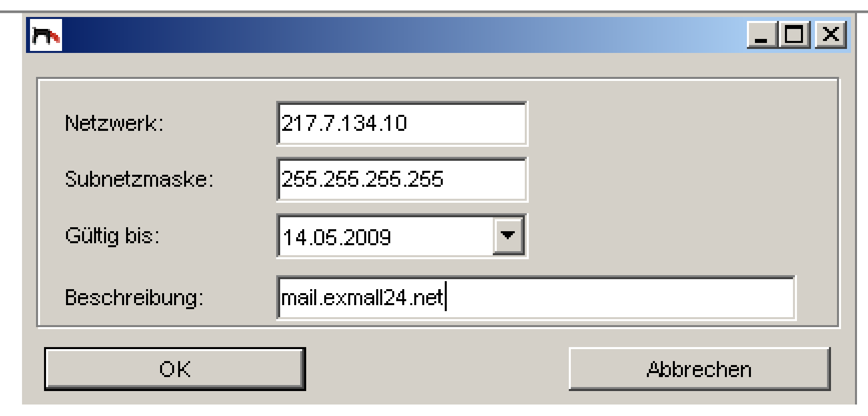



Abbildung: Zugelassene IP Adresse

4. Geben Sie das freizugebende Netzwerk oder eine einzelne IP-Adresse ein.
5. Geben Sie die zugehörige Subnetmaske an.
6. Geben Sie ein Gültigkeitsdatum ein. Nach Ablauf des Datums wird dieser Eintrag nicht mehr berücksichtigt.
7. Optional können Sie einen Grund für die Zulassung im Feld Beschreibung eintragen.
8. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**HINWEIS**

Ist die „dynamische IP Blacklist-Funktion" aktiviert, werden die zugelassenen IP-Adressen, bei Adressgleichheit in der gesperrten Adressliste, gelöscht. Um das zu verhindern, müssen Sie die Funktion deaktivieren, den Eintrag in der gesperrten Adressliste manuell entfernen, in die Liste der zugelassenen Adressen wieder eintragen und danach den SMTP-Server neu starten.

### 4.2.4.5 Gesperrte IP-Adressen

Um einzelne IP-Adressen oder komplette Netzabschnitte den SMTP-Verbindungsaufbau zu verbieten, können diese Adressen hier eingetragen werden. Des Weiteren werden über die *dynamische IP-Blacklist-Funktion* IP-Adressen von Mailservern, die auf einer Blacklist stehen, hier automatisch hinzugefügt. Diese haben eine Gültigkeit von einem Tag haben und werden nach Ablauf wieder automatisch gelöscht.

**Gesperrte IP Adresse neu anlegen**

1. Wählen Sie in der Baumansicht unter ***SMTP Konfiguration – Gesperrte IP-Adressen*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**
   Folgende Felder werden angezeigt:

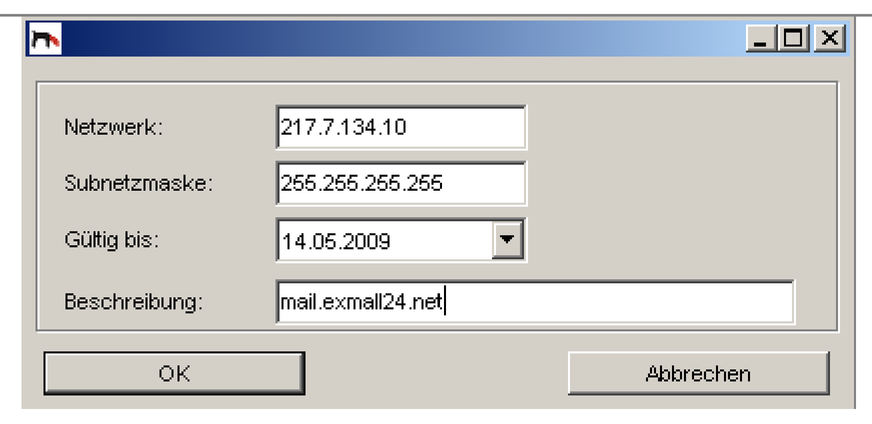



Abbildung: Gesperrte IP Adresse

4. Geben Sie das zu sperrende Netzwerk oder eine einzelne IP-Adresse ein.
5. Geben Sie die zugehörige Subnetmaske an.
6. Geben Sie ein Gültigkeitsdatum ein. Nach Ablauf des Datums wird dieser Eintrag nicht mehr berücksichtigt.
7. Optional können Sie einen Grund für die Sperrung im Feld Beschreibung eintragen.
8. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

## 4.2.5 Backup and Restore

**Informationen zum Backup**

Das Backup bietet die Möglichkeit die kompletten Daten der Appliance zeitgesteuert zu sichern. Dabei werden sämtliche Warteschlangen und alle Konfigurationen, sowie das gesamte Betriebssystem der REDDOXX Appliance gesichert.

### 4.2.5.1 Backup Einstellungen

**Netzwerkfreigabe einstellen**

Über die Freigabe können Sie den Netzwerkpfad angeben, in welchem das Backup gespeichert werden soll.

1. Wählen Sie in der Baumansicht unter ***Backup und Restore – Backup Einstellungen*** aus.
2. Klicken Sie mit der rechten Maustaste auf ***„Backup Einstellungen“***
3. Wählen Sie in der Auswahlliste den Eintrag ***Bearbeiten***
   Folgende Felder werden angezeigt:

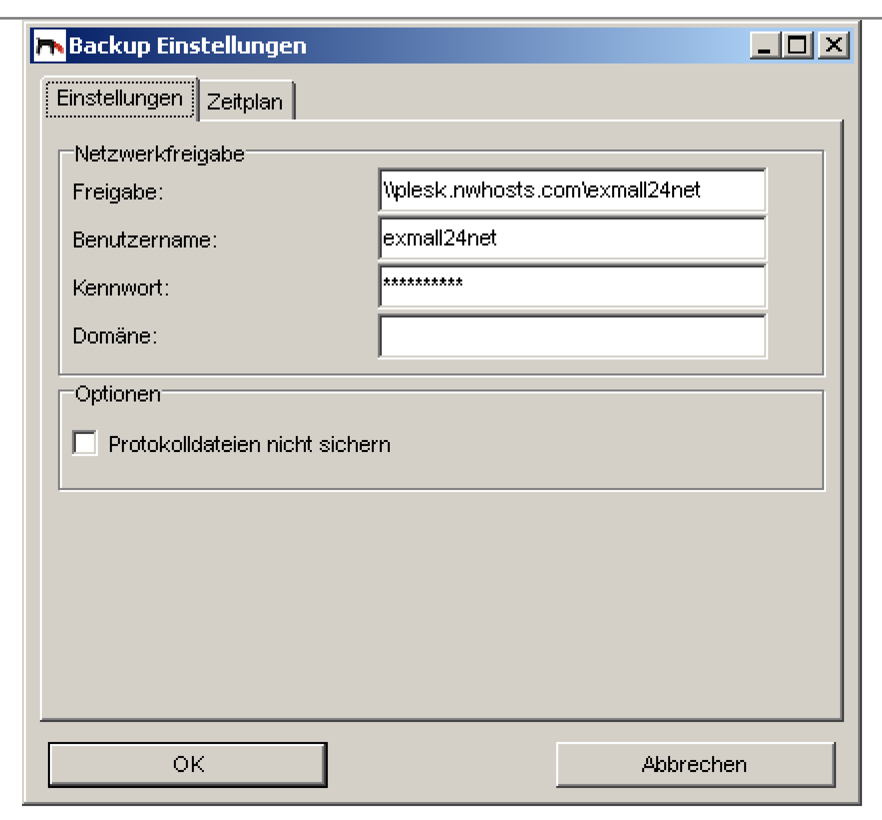



Abbildung: Backup Einstellungen

**Netzwerkfreigabe**

4. *Freigabe:*
   Geben Sie den UNC-Pfad an.

**HINWEIS**

Der Pfad wird im UNC (Uniform Naming Convention) im Format angegeben:
**\\servername\ordnername**

Es dürfen keine Unterverzeichnisse angeben werden!
Das Backup darf nicht zusammen mit einem anderen Verzeichnis (z.B. Archiv) zusammengelegt werden.

5. *Benutzername:*
   Geben Sie den Benutzernamen an.
6. *Kennwort:*
   Geben Sie das Kennwort an.
   **Das Kennwort darf nicht länger als 16 Zeichen sein!**
7. *Domäne:*
   Geben Sie eventuell den Namen der Domäne an.

**Optionen**

8. *Protokolldateien nicht sichern:*
   Sofern aktiviert, werden die Protokolldateien beim Backup nicht mitgesichert..

**Zeitplan einstellen**

Hier können Sie die Wochentage, die Zeit zu der das Backup gestartet werden soll und den Namen der Backupdatei eintragen. Erst wenn die Checkbox des Wochentages aktiviert ist, wird zur angegebenen Zeit das Backup im zuvor konfigurierten UNC-Pfad gespeichert.

**Voraussetzung:** Anmelden an der Administrator-Konsole der REDDOXX.

9. Wählen Sie in der Baumansicht unter ***Backup und Restore – Backup Einstellungen*** aus.
10. Klicken Sie mit der rechten Maustaste auf ***„Backup Einstellungen“***
11. Wählen Sie in der Auswahlliste den Eintrag ***Bearbeiten***
12. Klicken Sie auf den Reiter "Zeitplan".
    Folgende Felder werden angezeigt:

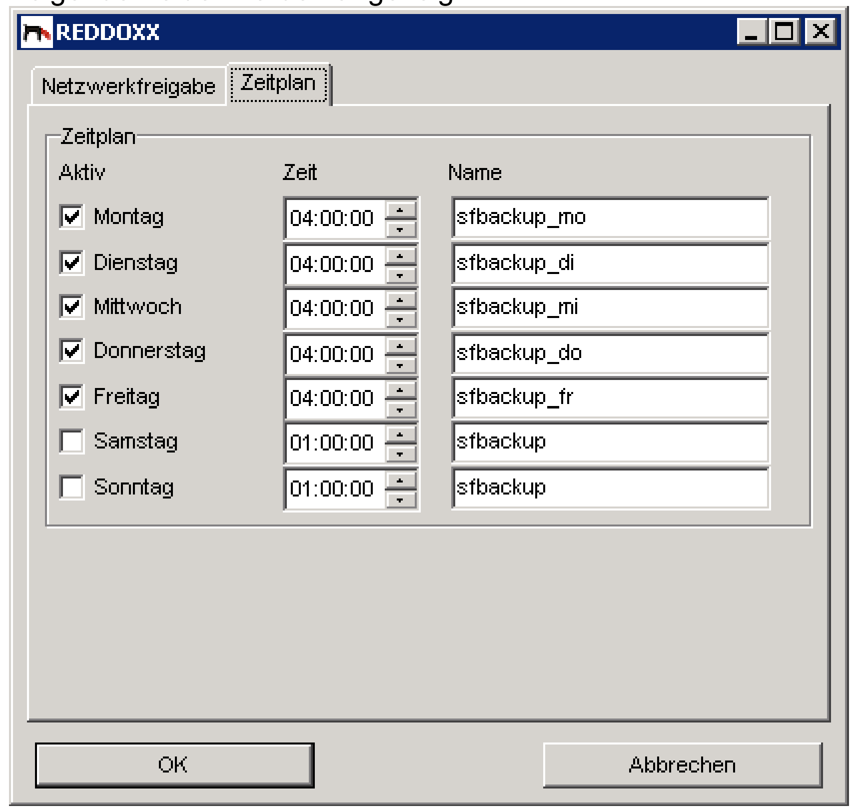



Abbildung: Backup Konfiguration - Zeitplan

**HINWEIS**

Sie können die Verbindung zur Server-Freigabe testen, indem Sie auf RESTORE klicken. Dabei darf keine Fehlermeldung in der Protokollansicht erscheinen. Bereits vorhandene Backups werden in der Listenansicht angezeigt.

### 4.2.5.2 Backups

In der Listenansicht sind die bisher geschriebenen Backups aufgeführt. Den Restore müssen Sie über die Appliance-Konsole vornehmen.

**HINWEIS**

Ab der Appliance Version 1021 kann der Restore nur noch über die Appliance Konsole ausgeführt werden. Siehe dazu im Kapitel 6.2 – Appliance Konsole - Backup und Restore

1. Mit einem Klick im Navigationsbaum auf BACKUP und RESTORE – BACKUPS werden die vorhanden Backup-Sets aufgelistet. Zum Wiederherstellen eines Backups verfahren Sie wie unter Kapitel 6.2 beschrieben.

Werden keine Backups angezeigt und erscheint im Live-Protokoll eine rote Fehlermeldung, ist der Zugriff auf die Netzwerkfreigabe gestört. Überprüfen Sie dann die Konfiguration.

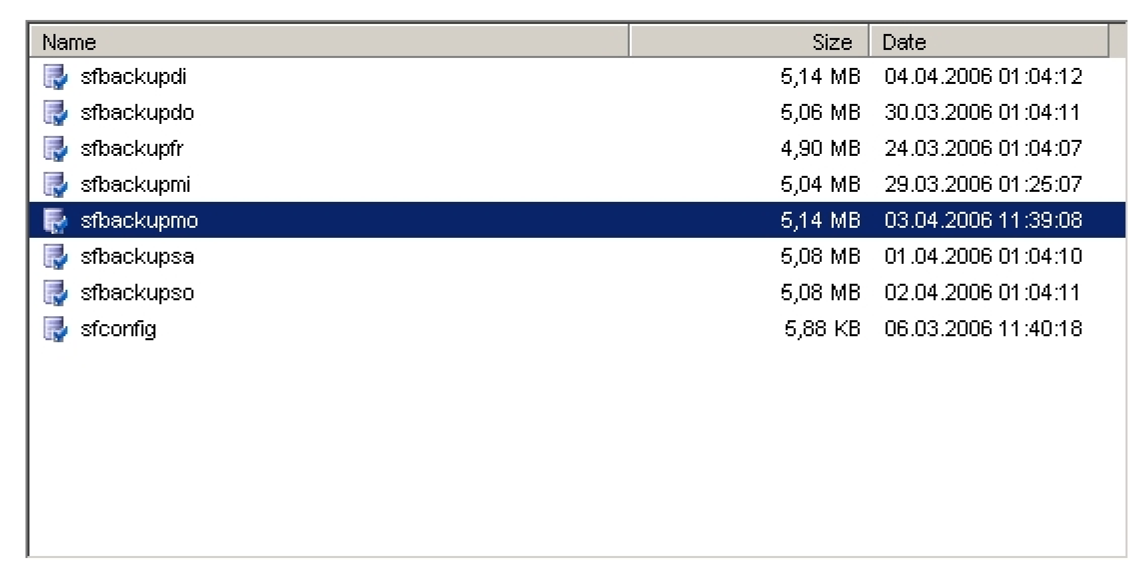



Abbildung: Backup und Restore – Backups

## 4.3 Appliance Administration

### 4.3.1 Nachrichten-Warteschlangen

**Informationen zu Warteschlangen**

In den Warteschlangen warten E-Mails auf die weitere Bearbeitung durch die REDDOXX Appliance.

**Funktionsweise**

**Siehe auch:** "Informationen zu den Diensten in Kapitel 4.3.7".

**Die ausgehenden und eingehenden Nachrichten sind die grundlegenden Warteschlangen der REDDOXX Appliance.**

#### 4.3.1.1 Eingehende Nachrichten

Vom SMTP-Server der REDDOXX Appliance angenommene E-Mails, die von intern bzw. extern versendet werden, werden temporär in der Warteschlange *Eingehende Nachrichten* abgelegt. Hier werden die E-Mails von der REDDOXX Appliance geprüft und je nach Ergebnis in den Warteschlangen Spam, CISS, Virus oder Ausgehende Nachrichten abgelegt.

In dieser Warteschlange können Sie E-Mails manuell suchen und löschen. In der Listenansicht sehen Sie die ID, die Empfangszeit, den Sender und Empfänger, die Größe, die Zustellungszeit sowie das Ergebnis der E-Mails. Auch das Sortieren über die Merkmale der E-Mails ist hier möglich.

### 4.3.1.2 Ausgehende Nachrichten

Alle E-Mails, die vom SMTP-Client der REDDOXX Appliance von intern bzw. extern versendet werden, werden in der Warteschlange *Ausgehende Nachrichten* abgelegt.
Weitere Informationen können Sie unter *Eingehende Warteschlangen* finden.

**E-Mail suchen**

In den jeweiligen Warteschlangen können Sie E-Mails suchen.
**Einschränkung:** Keine, suchen der E-Mails in allen Warteschlangen möglich.

1. Wählen Sie in der Baumansicht *Nachrichten-Warteschlange* oder *Spamfinder-Warteschlangen* mit einem Doppelklick aus.
2. Wählen Sie die gewünschte Warteschlange aus.
3. Klicken Sie in der Menüansicht das Symbol mit der Lupe.
4. Folgende Felder werden über der Liste angezeigt:




6. Geben Sie bei *Suchbegriff*, *Absender* und *Empfänger* die Ihnen bekannten Daten ein.
7. Auch das Sortieren über die Merkmale der E-Mails ist hier möglich. Klicken Sie dazu auf die Spaltenüberschrift. Erneutes Klicken kehrt die Reihenfolge um.
8. Klicken Sie SUCHE, um die Suche zu starten.

**E-Mail löschen**

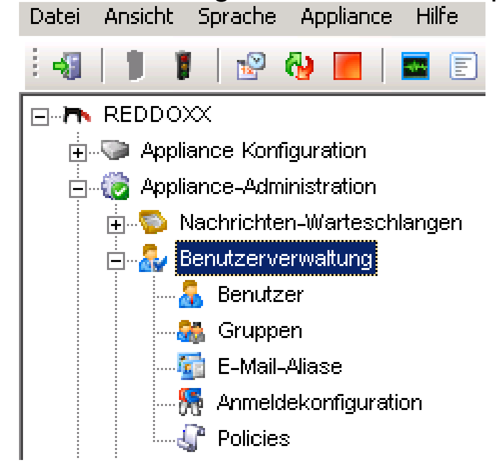
In den jeweiligen Warteschlangen können Sie E-Mails löschen.
**Einschränkung:** Keine. Löschen der E-Mails in allen Warteschlangen möglich.

1. Wählen Sie in der Baumansicht ***Warteschlangen*** mit einem Doppelklick aus.
2. Wählen Sie die gewünschte Warteschlange aus.
3. Klicken Sie die zu löschende E-Mail mit der rechten Maustaste an.
4. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
5. Bestätigen Sie die Sicherheitsabfrage mit JA, um die E-Mail zu löschen.
   NEIN: E-Mail wird nicht gelöscht.

## 4.3.2 Benutzerverwaltung

**Informationen zur Benutzerverwaltung**

In der Benutzerverwaltung können Sie Benutzer, lokale E-Mail-Adressen, die Anmeldekonfiguration, sowie Gruppen und Policies verwalten.



### 4.3.2.1 Benutzer

Unter der Rubrik *BENUTZER* können Sie Benutzer hinzufügen, bearbeiten, löschen, suchen und importieren, sowie Lizenzen zuteilen oder entziehen und das Kennwort ändern.
In der Listenansicht sind auf einen Blick folgende Daten ersichtlich:

- Liste mit Namen der angelegten Benutzer
- Primäre E-Mail-Adresse
- Realm
- Spamfinder-Lizenzen
- Archiv-Lizenzen
- MailSealer-Lizenzen

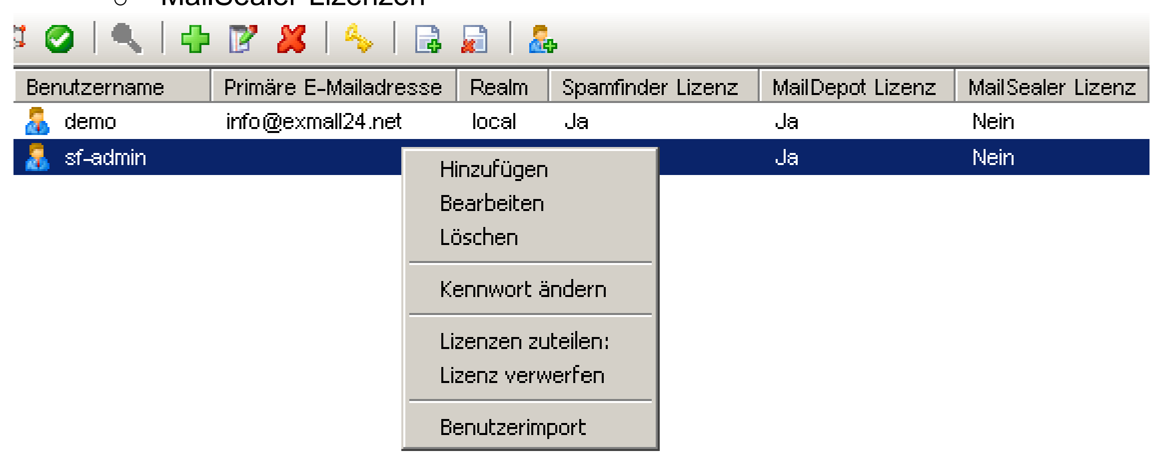



Abbildung: Benutzerverwaltung – Benutzer

**Benutzer hinzufügen**

1. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**.
   Folgende Felder werden angezeigt:

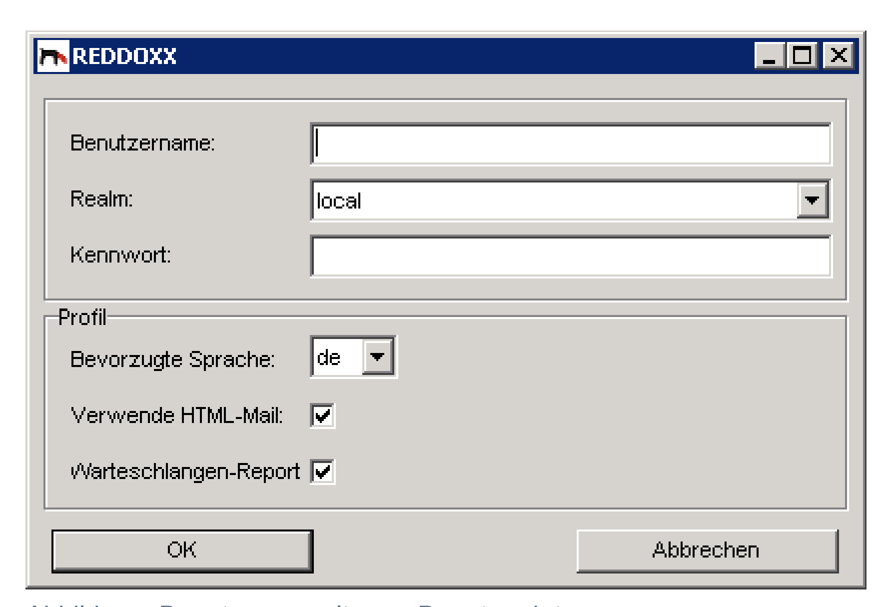



Abbildung: Benutzerverwaltung - Benutzerdaten

2. Geben Sie den gewünschten *Benutzername* an.
3. Wählen Sie einen Realm aus. Es stehen nur LOKALE Realms zur Auswahl.

**HINWEIS**

REALMS, die per LDAP-Konfiguration angegeben wurden, können hier nicht ausgewählt werden. Benutzer eines Remote-Realms werden automatisch angelegt, sobald der User sich an der Userkonsole anmeldet, oder er erstmals eine E-Mail bekommt.

4. Geben Sie ein Kennwort ein.
5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Benutzer bearbeiten**

Um einen bereits bestehenden Benutzer zu bearbeiten, gehen Sie wie folgt vor.

1. Klicken Sie den zu bearbeitenden Benutzer doppelt an.
   Das Fenster für die Konfiguration öffnet sich
2. Nehmen Sie alle gewünschten Änderungen vor.
3. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Benutzer löschen**

Um einen bereits bestehenden Benutzer zu löschen, gehen Sie wie folgt vor.

1. Klicken Sie den zu löschenden Benutzer mit der rechten Maustaste an.
2. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
3. Bestätigen Sie die Sicherheitsabfrage mit JA, um den ausgewählten Benutzer zu löschen. NEIN: Benutzer wird nicht gelöscht.

**Kennwort einstellen**

Um das Kennwort eines Benutzers zu ändern, gehen Sie wie folgt vor.

1. Klicken Sie in der Listenansicht auf einen Benutzer mit der rechten Maustaste.
2. Wählen Sie in der Auswahlliste den Eintrag **Kennwort einstellen**.
   Folgendes Fenster erscheint:

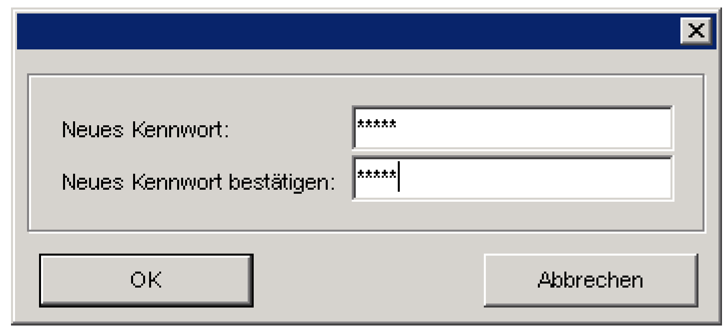



Abbildung: Benutzerverwaltung – Kennwort einstellen

3. Geben Sie das neue Kennwort ein.
4. Bestätigen Sie das neue Kennwort.
5. Klicken Sie auf OK. Das neue Kennwort wurde gesetzt. Der Dialog wird geschlossen.

### Lizenz zuteilen

Um Benutzern eine Lizenz zuzuteilen, gehen Sie wie folgt vor.

1. Markieren Sie in der Listenansicht einen oder mehrere Benutzer mit der rechten Maustaste und wählen Sie „Lizenz zuteilen“.
2. Folgender Dialog geht auf:

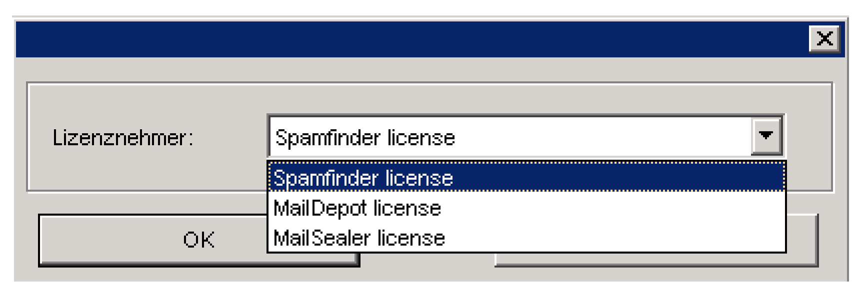



Abbildung: Benutzerverwaltung – Lizenzen zuteilen

3. Wählen Sie in der Auswahlliste den Eintrag „Spamfinder-Lizenzen“, „Archiv-Lizenzen“ oder MailSealer-Lizenzen und klicken Sie auf OK.
   Das Dialogfenster wird geschlossen. Die Lizenzen wurden zugeteilt und sind sofort, ohne Neustart, aktiv.

### Lizenz verwerfen

Um Benutzern eine Lizenz wegzunehmen, gehen Sie wie zuvor beschrieben vor. Wählen sie zu Beginn aber im Kontextmenü die Option „Lizenz verwerfen“ Auch hier ist die Mehrfachselektion möglich.

**HINWEIS**

Lizenzen werden bei Nutzung des Spamfinders oder des Maildepots in der Userkonsole automatisch zugeteilt. Ab Version 1021 werden die zugeteilten Lizenzen geprüft. Wurden zuvor bereits Lizenzen zugeteilt, kann es vorkommen, dass nach einem Firmware-Update auf Version 1021 oder höher die Anzahl der zur Verfügung stehenden Lizenzen bereits überschritten sind und die Fehlermeldung „Invalid license count“ oder „no valid license“ im Protokoll erscheint. Sie können dann hier pro Benutzer Lizenzen verwerfen (siehe auf FAQ).

### Benutzer importieren

Um Benutzer aus einer Liste zu importieren, gehen Sie wie folgt vor.

1. Klicken Sie in der Listenansicht die rechte Maustaste.
2. Wählen Sie in der Auswahlliste den Eintrag **Benutzerimport**.
   Folgendes Fenster erscheint:

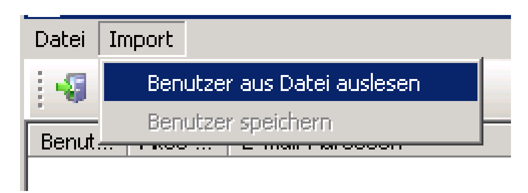



Abbildung: Benutzerverwaltung – Benutzerimport

3. Wählen Sie im Menü *Import* die Option *Benutzer aus Datei auslesen*.

**HINWEIS**

Die Import-Datei muss folgende Struktur aufweisen:

**Benutzername,Kennwort,Realm,E-Mail-Adresse1,E-Mail-AdresseN …**

Falls keine Benutzer in der Liste angezeigt werden, prüfen Sie folgende Einschränkungen:
- Felder müssen mit Komma separiert werden.
- Benutzer müssen eindeutig sein.
- Alle Felder dürfen nicht leer sein. (auch nicht das Kennwort!)

4. Wählen Sie die Importdatei aus und klicken Sie auf ***öffnen***. Es erscheint die Importliste.

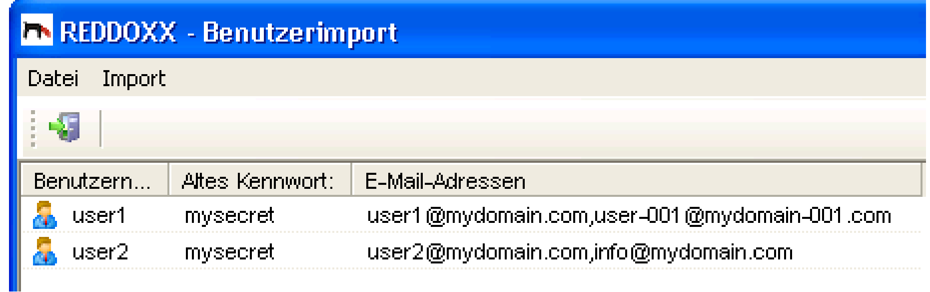



Abbildung: Benutzerverwaltung – Benutzerimport – Benutzerliste

5. Im Menü **Import** wählen Sie **Benutzer speichern**.
   Folgender Dialog erscheint:

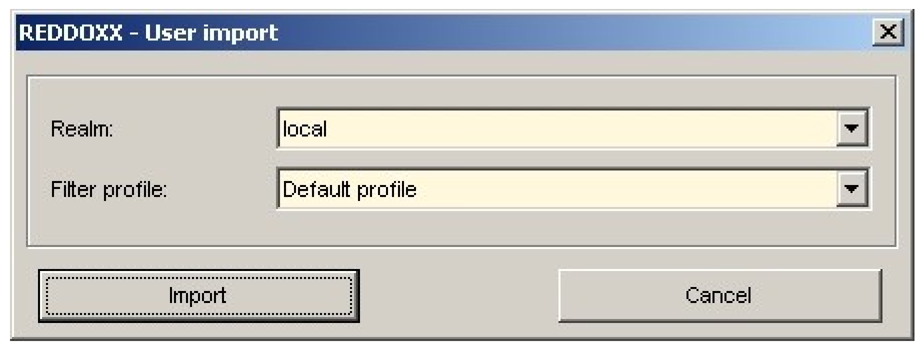



Abbildung: Benutzerverwaltung – Benutzerimport – Filterauswahl

6. Wählen Sie den **Realm** und das zu verwendende Profil für die zu importierenden Benutzer aus.
7. Wenn die Benutzer erfolgreich importiert wurden, können Sie das Fenster schließen. Die Benutzer erscheinen in der Listenansicht.

### 4.3.2.2 Gruppen

Gruppen sind zur Steuerung der Benutzer-Richtlinien (Policies) erforderlich. Einer Gruppe werden ein oder mehrere Benutzer zugeordnet.
In der Listenansicht sehen Sie die Spalten *Gruppenname* und *Beschreibung*. Sie können Gruppen hinzufügen, bearbeiten und löschen.

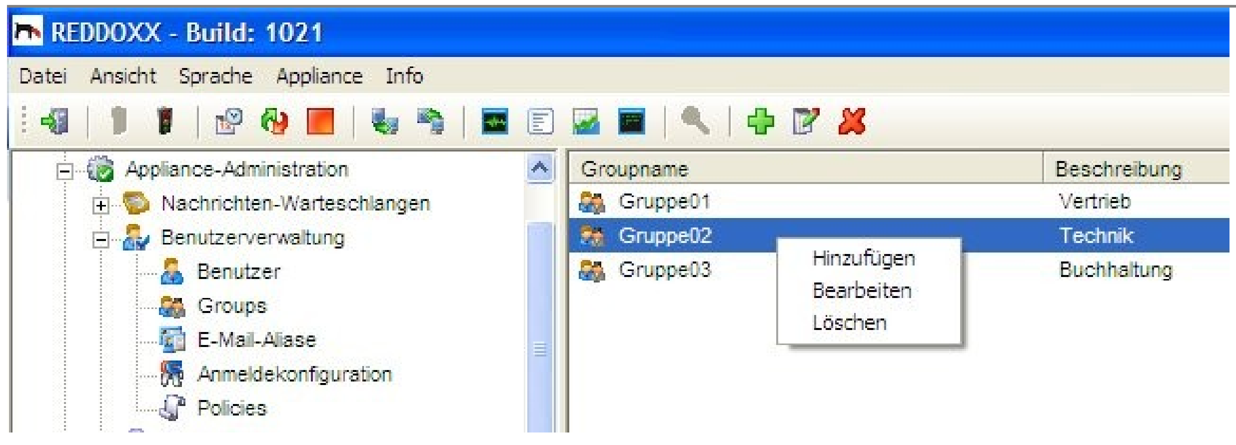



Abbildung: Benutzerverwaltung – Gruppen

### Gruppe hinzufügen

1. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**.
   Folgender Dialog wird angezeigt:

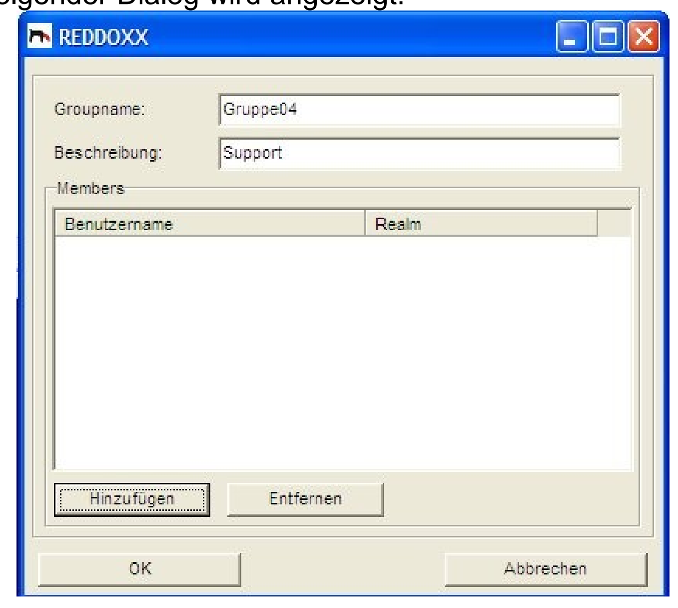



Abbildung: Benutzerverwaltung – Gruppe hinzufügen

2. Geben Sie einen Gruppennamen an.
3. Geben Sie eine Beschreibung an.
   Klicken Sie auf HINZUFÜGEN, um Benutzer dieser Gruppe zuzuordnen.
   Folgender Dialog wird angezeigt:

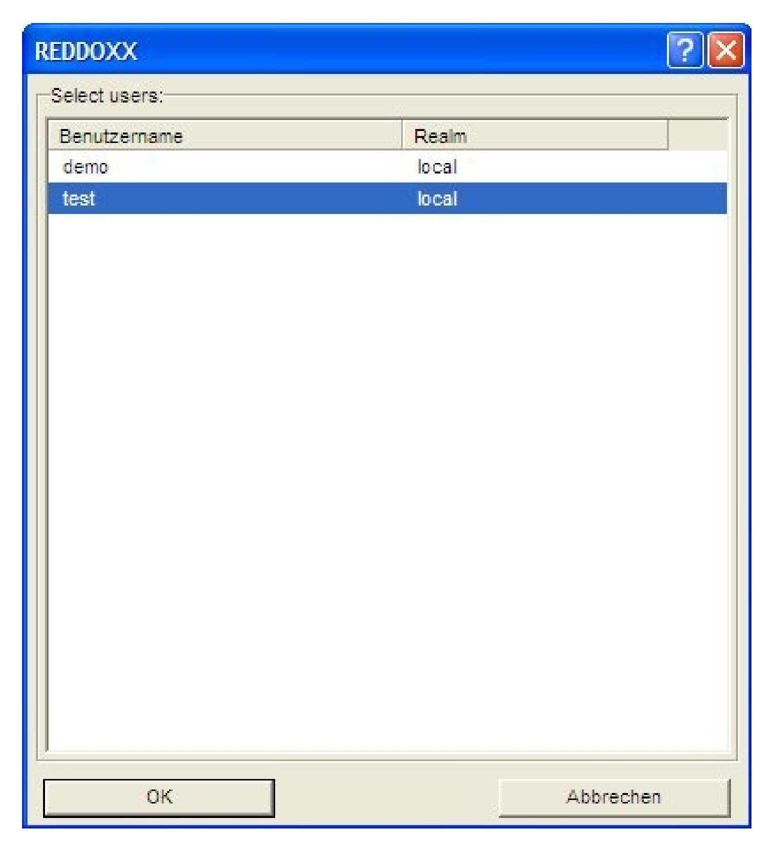



Abbildung: Benutzerverwaltung – Benutzer zur Gruppe hinzufügen

4. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.
5. Klicken Sie auf OK, um die Benutzer-Gruppenzuordnung zu übernehmen.
6. Klicken Sie auf OK, um die Gruppe nun anzulegen.

**Gruppe bearbeiten**

1. Klicken Sie die zu bearbeitende Gruppe doppelt an.
2. Nehmen Sie alle gewünschten Änderungen vor.
3. Klicken Sie auf OK.

**Gruppe löschen**

1. Klicken Sie mit der rechten Maustaste auf die zu löschende Gruppe.
2. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.

Bestätigen Sie die Sicherheitsabfrage mit JA, um die ausgewählte Gruppe zu löschen. NEIN: Die Gruppe wird nicht gelöscht.

#### 4.3.2.3 E-Mail-Aliase

E-Mail-Aliase werden einem Benutzer zugeordnet. Sie können E-Mail-Aliase hinzufügen, bearbeiten, löschen, für mehrere E-Mail-Aliase zugleich das Filterprofil ändern und die Archivierung dieser E-Mailadressen verhindern (deaktivieren).
In der Listenansicht sehen Sie die Spalten *E-Mail-Adresse, Filterprofil*, *Benutzer und Archivierung deaktivieren*.

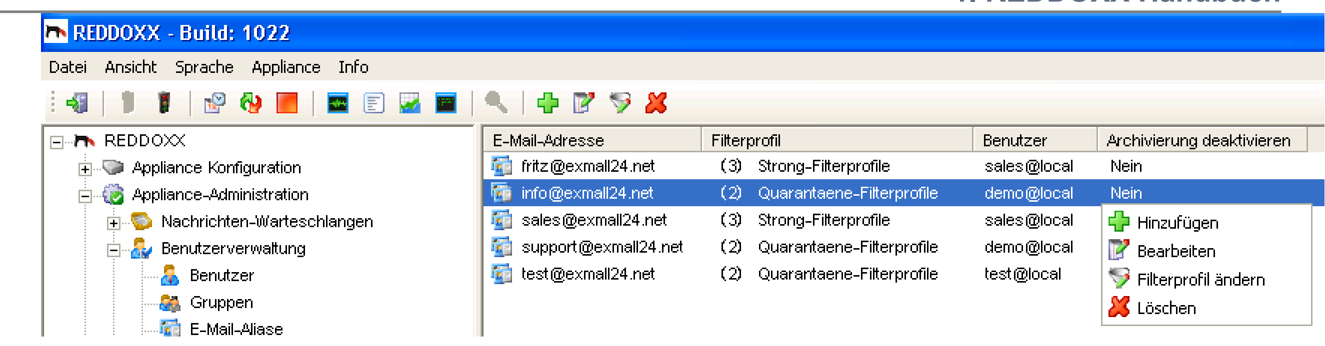



Abbildung: Benutzerverwaltung – E-Mail-Aliase

## E-Mail-Alias hinzufügen

1. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**.
   Folgende Felder werden angezeigt:

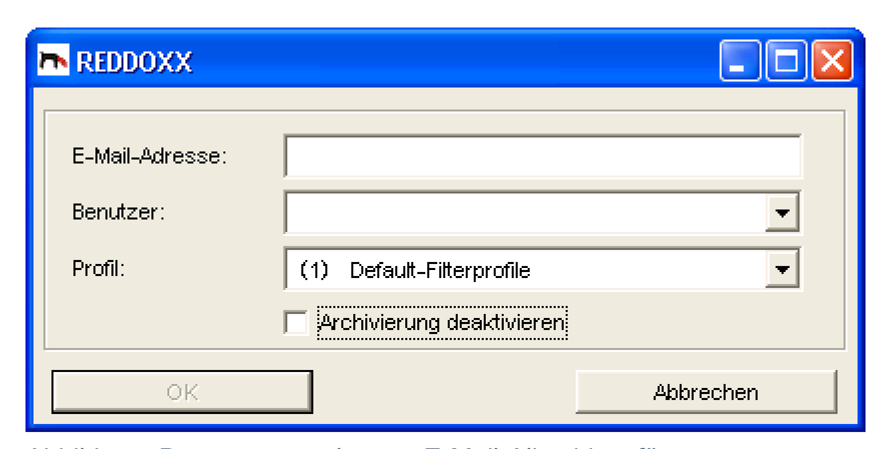



Abbildung: Benutzerverwaltung – E-Mail-Alias hinzufügen

2. Geben Sie die gewünschten ***E-Mail-Adresse*** an.
3. Wählen Sie den **Benutzer** aus, der diese Adresse verwalten darf.
4. Wählen Sie ein gewünschtes Filterprofil aus.
5. Wählen Sie die Option ***Archivierung deaktivieren***, wenn Sie das Archivieren dieser E-Mails verhindern wollen.
6. Klicken Sie OK, um den E-Mail-Alias nun anzulegen.

## E-Mail-Aliase bearbeiten

1. Klicken Sie die zu bearbeitende **E-Mail-Adresse** doppelt an.
   Folgender Dialog wird angezeigt:

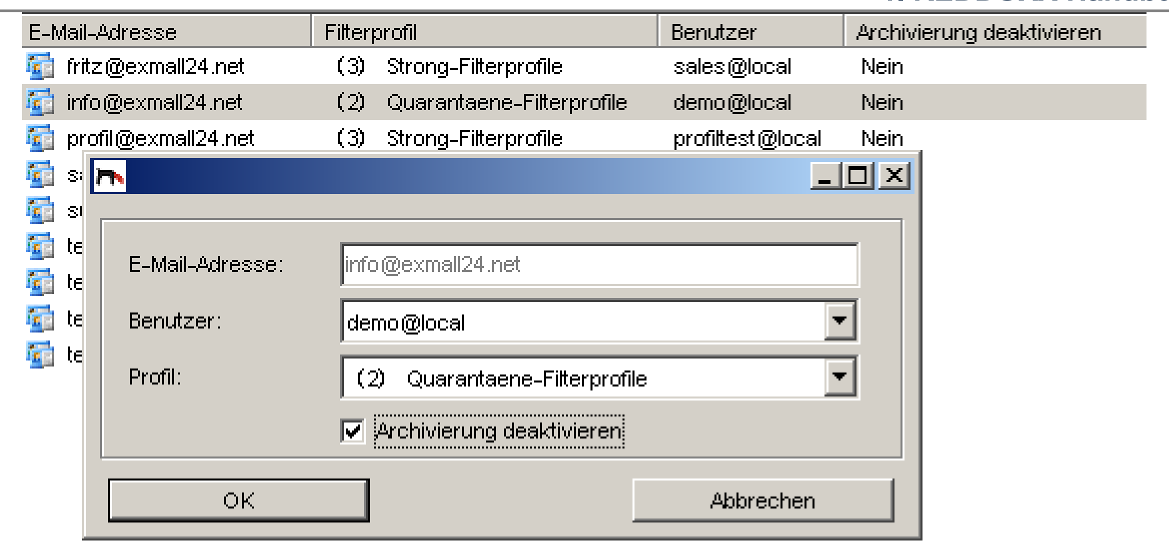



Abbildung: Benutzerverwaltung - E-Mail-Adresse

2. Benutzer: Sie können an dieser Stelle den E-Mail-Alias einem anderen Benutzer zuordnen.
3. Profil: Ordnen Sie der E-Mail-Adresse ein anderes Filter-Profil zu
4. Archivierung deaktivieren: Aktivieren Sie diese Checkbox, wenn Sie die Archivierung aller E-Mails an diese Adresse unterbinden wollen.
5. Klicken Sie auf **OK**, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**E-Mail-Aliase löschen**

1. Klicken Sie mit der rechten Maustaste auf den zu löschende E-Mail-Alias.
2. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
3. Bestätigen Sie die Sicherheitsabfrage mit JA, um die ausgewählte E-Mail-Adresse zu löschen. NEIN: E-Mail-Alias wird nicht gelöscht.

**Filterprofile ändern**

1. Markieren Sie alle E-Mail-Aliase, bei denen Sie das Filterprofil gleichzeitig ändern möchten.
2. Klicken Sie auf der Listenauswahl rechts. Folgender Dialog geht auf:

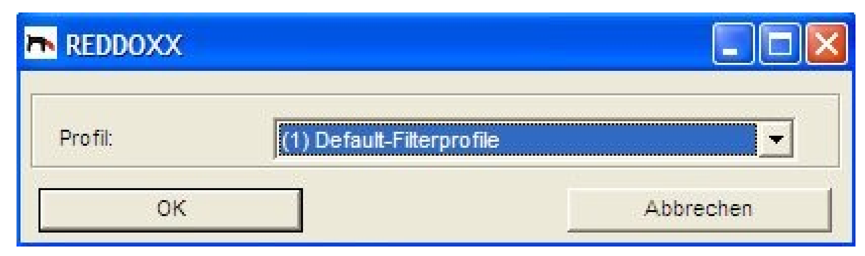


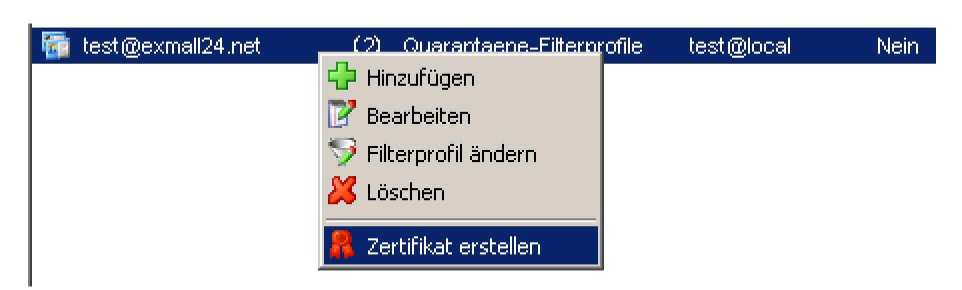

Abbildung: Benutzerverwaltung – Filterprofil ändern

3. Wählen Sie das gewünschte Filterprofil aus.
4. OK: Alle zuvor ausgewählten E-Mail-Aliase bekommen das neu eingestellte Filterprofil zugeordnet.

**Zertifikat erstellen**

Voraussetzungen: Das REDDOXX CA Root-Zertifikat muss vorhanden sein.

1. Markieren Sie alle E-Mail-Aliase, für die Sie ein Zertifikat erstellen möchten.
2. Klicken Sie mit der rechten Maustaste. Folgendes Kontextmenü wird angezeigt:




3. Wählen Sie „Zertifikat erstellen“ aus. Sie können in der Protokollanzeige verfolgen, ob und für wen ein Zertifikat erstellt wurde. Bereits vorhandene Zertifikate werden überschrieben (neu ausgestellt).




### 4.3.2.4 Anmeldekonfiguration

Die Anmeldekonfiguration legt fest, welche Benutzerdatenbank zur Autorisierung der Benutzer verwendet wird. Sie können mehrere Anmeldekonfigurationen (Realms) festlegen, um die Anmeldung für den Benutzer aus verschiedenen Systemen zu ermöglichen.

Die Standard Anmeldekonfiguration „*local*“ benutzt die lokale Benutzerdatenbank der REDDOXX Appliance. Sie kann nicht gelöscht oder verändert werden.
Sie können Realms hinzufügen, bearbeiten und löschen.
In der Listenansicht sind sehen Sie die Spalten *Name* und *Authentifizierungsart*.

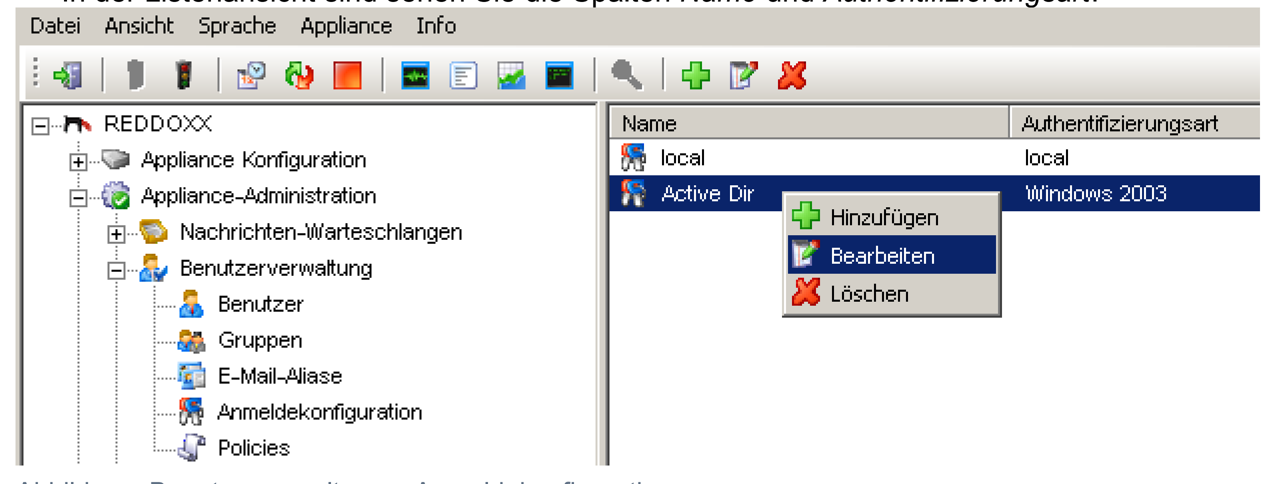



Abbildung: Benutzerverwaltung – Anmeldekonfiguration

**Realm neu anlegen**

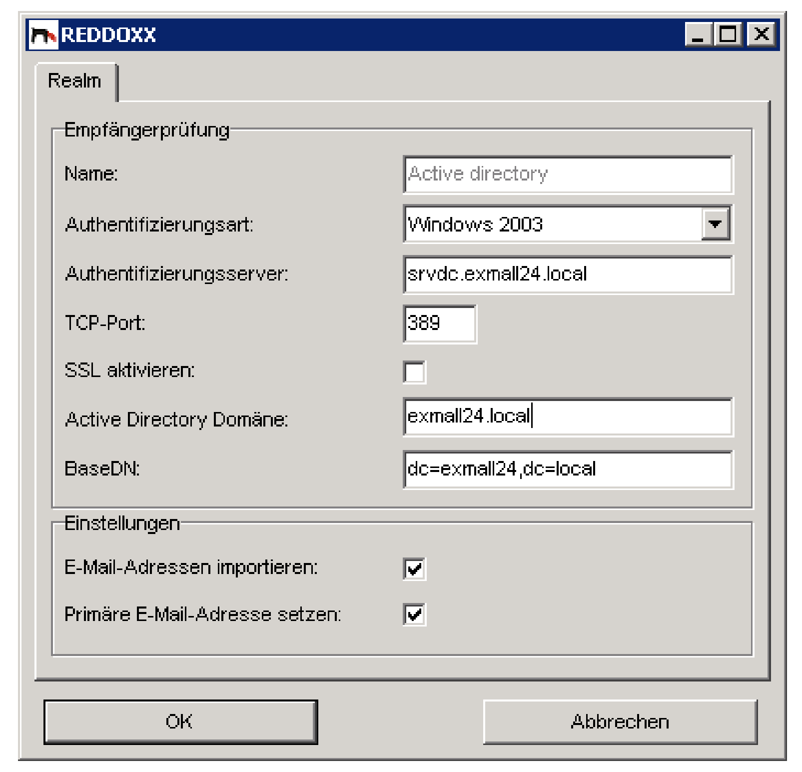



Abbildung: Benutzerverwaltung - Realm

1. Geben Sie den Realm *Name* an.
2. Wählen Sie über die Auswahlliste die **Authentifizierungsart** aus. Die Authentifizierungsart “local” verweist auf die lokale Benutzerdatenbank der REDDOXX Appliance.
3. Geben Sie den *Authentifizierungsserver* an.
   Unterstützt werden local, Windows2000, Windows2003, Netware5, Netware6 Active Directory, Lotus Domino, OpenLDAP.
4. Geben Sie den *TCP-Port* an. Der Default-Port für LDAP ist 389. Hier muss ein gültiger Wert eingetragen werden.
5. Aktivieren Sie bei Bedarf die Option *Sichere Übermittlung SSL*. Beachten Sie, dass der Default-Port für LDAP via SSL 636 ist.
6. Geben Sie die *Active Directory Domäne* an.
7. Geben Sie die *Base-DN* an.
8. *E-Mail-Adressen importieren:*
   Aktivieren Sie bei Bedarf die Option *E-Mail-Adressen importieren*, um bei jeder Benutzeranmeldung die E-Mail-Adressen für den Benutzer mit dem Authentifizierungsserver abzugleichen.
9. *Primäre E-Mail-Adresse setzen:*
   Aktivieren Sie bei Bedarf die Option *Primäre Adresse setzen*, um bei jeder Benutzeranmeldung die Primäre E-Mail-Adresse für den Benutzer mit dem Authentifizierungsserver abzugleichen.
10. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
    ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Realm bearbeiten**

1. Klicken Sie den zu bearbeitenden REALM doppelt an.
   Das Fenster für die Konfiguration öffnet sich.

2. Nehmen Sie alle gewünschten Änderungen vor.
3. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Realm löschen**

1. Klicken Sie den zu löschenden Realm mit der rechten Maustaste an.
2. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
3. Bestätigen Sie die Sicherheitsabfrage mit JA, um den ausgewählten Realm zu löschen.
   NEIN: Realm wird nicht gelöscht.

**HINWEIS - INFORMATIONEN ZUR ANMELDEKONFIGURATION**

Die Anmeldekonfiguration legt fest, welche Benutzerdatenbank zur Autorisierung der Benutzer verwendet wird.

In nachfolgender Tabelle finden Sie die unterstützen Systeme und den jeweiligen Funktionsumfang:

| LDAP-SERVER | USER AUTHENTICATION | RECIPIENT CHECK | USER AUTO CREATION | E-MAIL ADDRESS IMPORT |
|---|---|---|---|---|
| Microsoft Active Directory with Exchange 2000+ | Yes | Yes | Yes | Yes |
| Exchange 5.5 | No | Yes | No | No |
| Lotus Notes Domino 6+ | Yes | yes² | Yes | Yes² |
| Novell eDirectory | Yes | No | No | No |
| OpenLDAP | Yes | Yes | Yes | Yes |

² Für Lotus Notes Domino gelten folgende Einschränkungen:

Nur folgende E-Mail-Adressen werden als gültig gewertet:
- Internet address (Internetadresse)
- Shortname/UserID (Kurzname)
- User name (Benutzername)

Die angegebenen Adressen müssen im Lotus Domino eindeutig sein! Doppelte Einträge führen zum Ablehnen der E-Mail.
Bei Shortname/UserID kann die Internetdomäne weggelassen werden. Dann werden alle Internetdomänen, die im Dominoserver definiert sind, akzeptiert.
Beim Import während einer Benutzeranmeldung wird zuerst nur die Internet Address als E-Mail-Alias in der REDDOXX Appliance angelegt. Die weiteren E-Mail-Adressen werden dann beim E-Maileingang erstellt.

**Konfiguration:**

| | WINDOWS 2000 | WINDOWS 2003 | NETWARE 5.X | NETWARE 6.X |
|---|---|---|---|---|
| Authentifizierungsart | Windows 2000 | Windows 2003 | Netware 5 | Netware 6 |

| | | |
|---|---|---|
| Authentifizierungsserver | IP/Hostname eines Windows Domain Controller | IP/Hostname eines Netware-Servers mit LDAP Dienst |
| TCP-Port | TCP-Port des LDAP Dienstes Standard: 389 ODER für Secure-LDAP: 636 | |
| Sichere Übermittlung | Aktivieren Sie hier Secure-LDAP, falls Ihr System Secure-LDAP unterstützt. | |
| Active Directory Domain | AD-Domain, z.B. company.com | Wird nicht benötigt. |
| BaseDN | dc=company, dc=com | z.B. o=context |

| | LOTUS DOMINO | OPENLDAP |
|---|---|---|
| Authentifizierungsart | Windows 2000 | Windows 2003 |
| Authentifizierungsserver | IP/Hostname des Servers mit LDAP Dienst | |
| TCP-Port | 389 / SecureLDAP 636 | |
| Sichere Übermittlung | Aktivieren Sie hier Secure-LDAP, falls Ihr System Secure-LDAP unterstützt. | |
| Active Directory Domain | | |
| BaseDN | | o=REDDOXX,dc=company, dc=com |

**HINWEIS**

Für die LDAP-Anbindung an Novell Netware ist es erforderlich, dass die folgenden Benutzereigenschaften mit einem **anonymen LDAP-Bind** gelesen werden können: dn, cn, objectClass.

Weitere LDAP-Einstellungen können Sie im REDDOXX Support Center unter http://support.reddoxx.net in der Rubrik REDDOXX Download Center/Build1020 finden.

#### 4.3.2.5 Policies – Gruppenrichtlinien

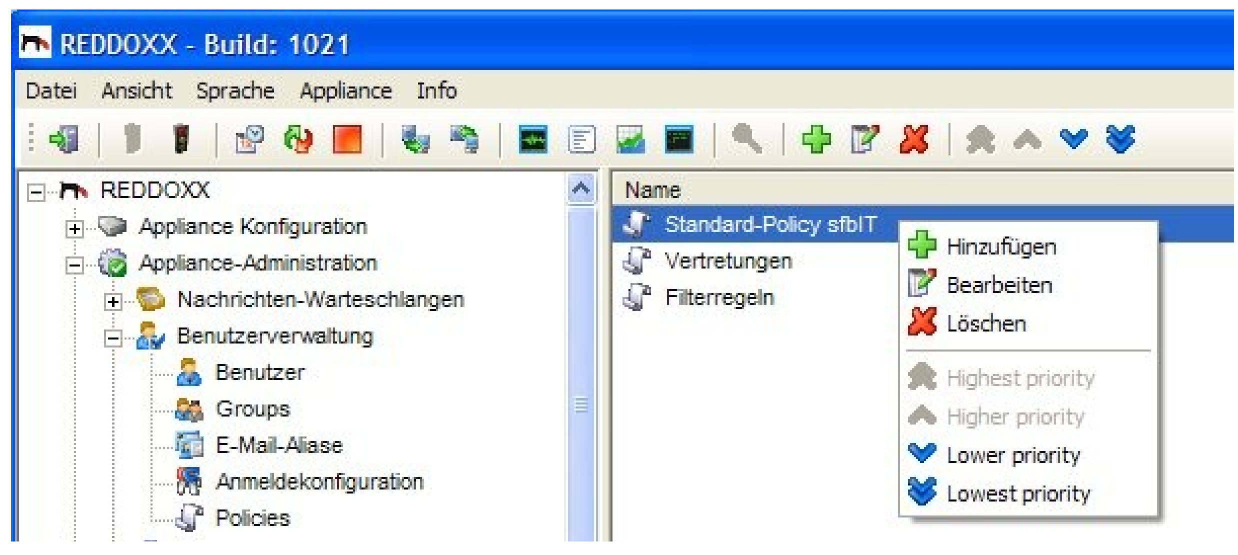



Abbildung: Benutzerverwaltung – Policies

**Funktionsüberblick und Begrifflichkeiten**
Mit den Policies können Sie Regeln erstellen, die den Funktionsumfang der Userkonsole bestimmen. Regeln werden dabei immer auf Gruppen angewendet. Voraussetzung ist daher, dass Sie bereits die Benutzer zu Gruppen zugeordnet haben (siehe Kapitel 4.3.2.2).
Mit den Policies wird festgelegt, ob ausgewählte Funktionen - für eine - oder mehrere Gruppen - erlaubt oder verboten sind.
**Beispiele**:
- Whitelist-Einträge hinzufügen / löschen
- E-Mails aus Warteschlangen löschen

In einer Policy gibt es sogenannte *Rule-Sets*, eine Zusammenfassung einzelner Funktionen zur einem Überbegriff.

**Rule-Sets**
Folgende Rule-Sets stehen zur Auswahl:
- Allgemeine Regeln
- Spamfinder Regeln
- Spamfinder Filterlist-Regeln
- Maildepot Regeln
- Mailsealer Regeln
- Stellvertreter-Gruppen

Ein Rule-Set kann 3 verschiedene Zustände haben:
1. Nicht konfiguriert
2. Deaktiviert
3. Aktiviert

Zu 1.) Dieses Regelwerk wird nicht ausgewertet. Es wird in dieser Policy ignoriert. Der Zustand der einzelnen Funktion bleibt unverändert.
Zu 2.) Alle Funktionen dieses Rule-Sets sind deaktiviert. Nachfolgende Policies werden für diese Rule-Set nicht mehr berücksichtigt.
Zu 3.) Die Funktionen des Rule-Sets werden einzeln berücksichtigt. Nachfolgende Policies werden für diese Rule-Set nicht mehr berücksichtigt.

**Funktionsablauf**
Sind noch keine Policies vorhanden, oder sind alle Rule-Set *nicht konfiguriert*, so gilt zuerst einmal der Default der Optionen und es sind keine Stellvertreter definiert.
Bei der Anmeldung des Benutzers an der Userkonsole werden alle vorhandenen Policies der Reihe nach, von oben nach unten, durchlaufen.
Ist ein Benutzer in der Gruppe enthalten, die der Policy zugeordnet wurde, so wird das Rule-Set in den nachfolgenden Policies nicht mehr berücksichtigt, es sei denn das Rule-Set hat zuvor den Status *nicht konfiguriert*.
Die Reihenfolge der Policies kann über das Kontextmenü eingestellt werden (höher, niedriger).

**Konfiguration der Rule-Sets**

1. Öffnen Sie das Fenster zum Bearbeiten der Konfiguration durch Rechtsklick auf einer Policy im Baum-Menü.

   Folgendes Fenster erscheint:

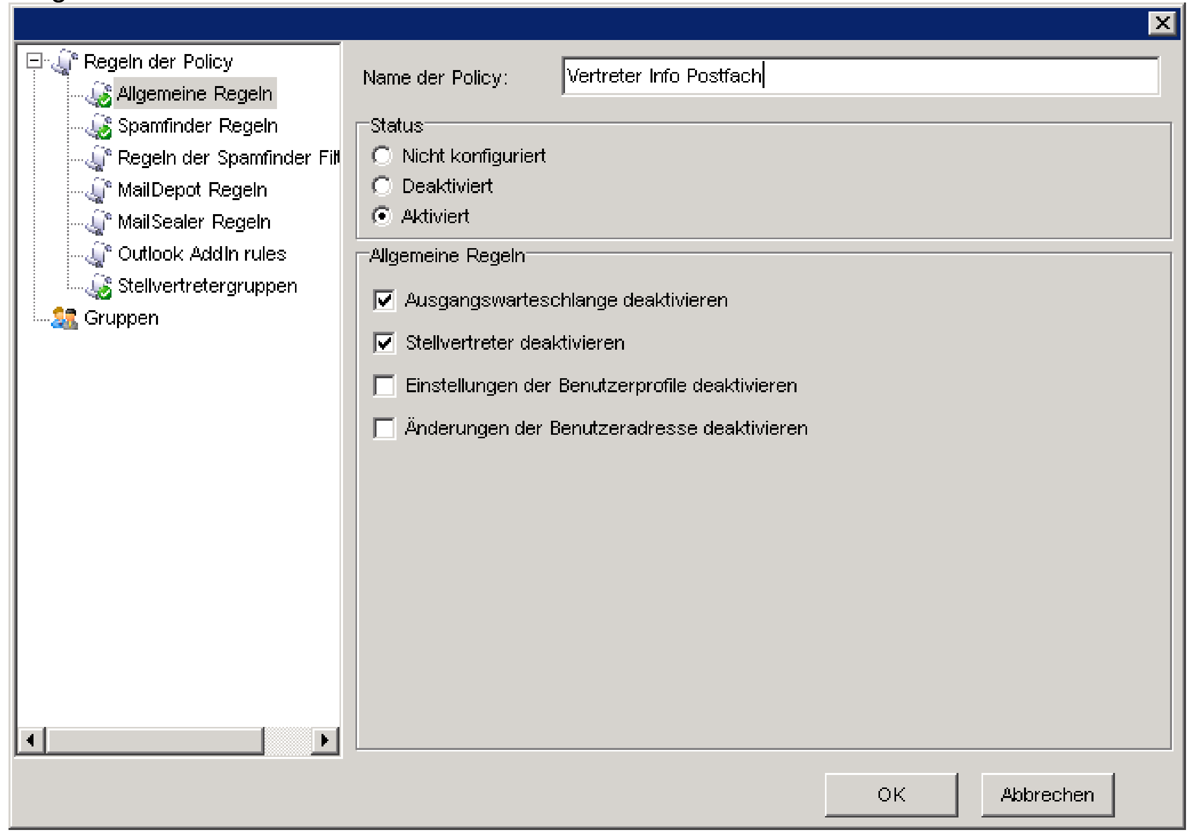



Abbildung: Policy Konfiguration

2. Wählen Sie das gewünschte Rule-Set aus und aktivieren Sie es.
3. Wählen Sie die Optionen aus, die Sie aktivieren möchten.

**Gruppenzuordnung**

4. Ordnen Sie diese Policy einer Gruppe zu.

**HINWEIS**

Policies gelten immer nur für diejenigen Benutzer, die in den Benutzer-Gruppen sind, die hier angegeben werden.

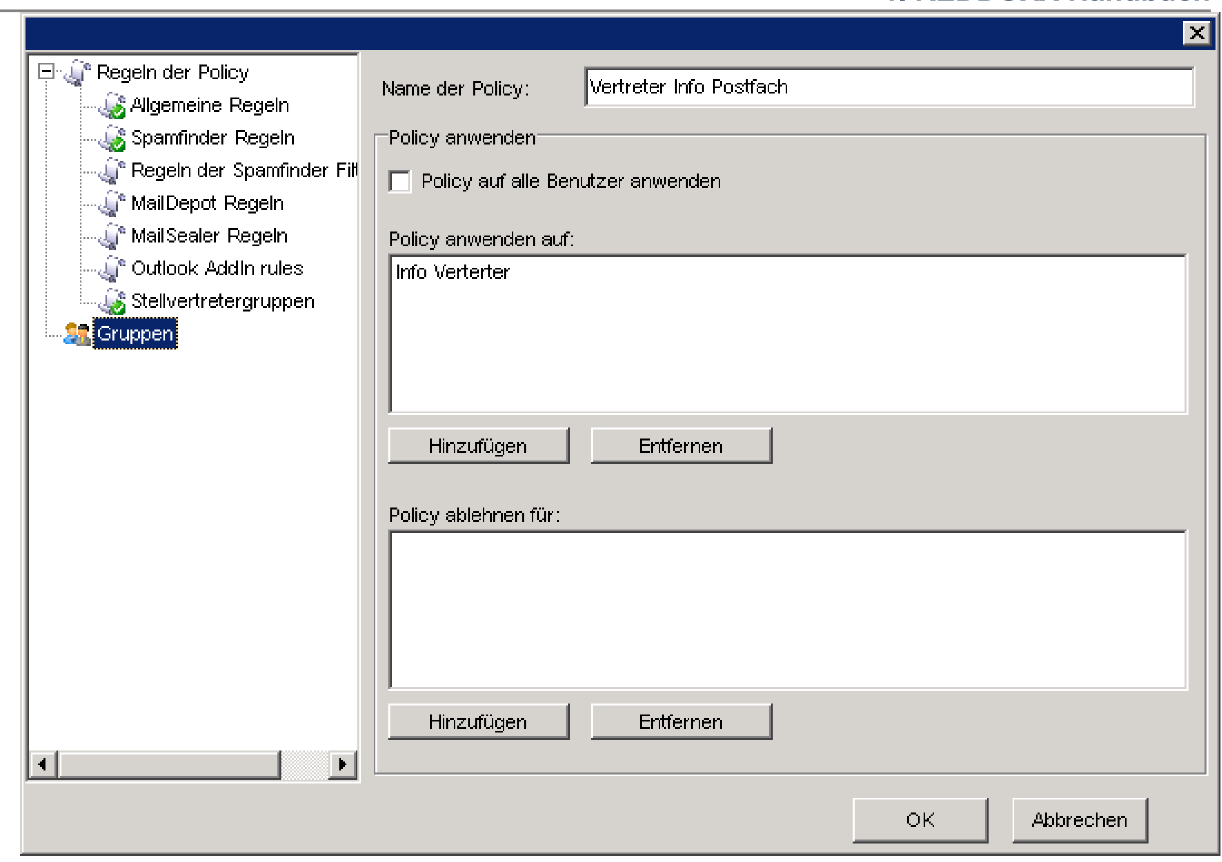



Abbildung: Policy Konfiguration

5. Checkbox *Policy auf alle Benutzer anwenden* ordnet diese Policy für alle Benutzer zu. Dies erübrigt die Konfiguration und Pflege einer Gruppe, die alle Benutzer beinhaltet.

**Eingabebereich *Policy anwenden auf*:**

6. *HINZUFÜGEN* fügt eine Gruppe aus einer Auswahlliste von Gruppen hinzu (siehe Kapitel 4.3.2.2).
   Das Rule-Set dieser Policy wird für Benutzer, die in diese Gruppe enthalten sind, angewendet.
7. *ENTFERNEN* entfernt eine markierte Gruppe aus dieser Policy.

**Eingabebereich *Policy ablehnen für*:**

*HINZUFÜGEN* fügt eine Gruppe zur Gruppen-Ausnahmeliste hinzu.
Das Rule-Set dieser Policy wird für Benutzer, die in diese Gruppe enthalten sind, NICHT angewendet.

8. Klicken Sie auf *OK* zum Abspeichern der Einstellungen.

**Stellvertreter**

Eine Besonderheit bei den Rule-Sets stellt das Stellvertreter-Gruppe-Rule-Set dar.
Hier kann der Administrator *Stellvertreter* für Benutzer zuordnen, die z.B. im Urlaub sind. Der Stellvertreter hat dadurch Zugang zu den E-Mails des Benutzers, der vertreten werden soll.
Im Rule-Set *Stellvertreter-Gruppen* wird definiert, welche E-Mail-Adressen vertreten werden können.

**HINWEIS**

Stellvertreter-Gruppen dienen lediglich der Übersichtlichkeit und haben keinen Zusammenhang mit den Benutzer-Gruppen.

In der Benutzer-Gruppenzuordnung der Policy wird bestimmt, wer diese E-Mail-Adressen (*Stellvertreter-Gruppen)* vertreten darf.

**Konfiguration der Stellvertreter-Gruppen**

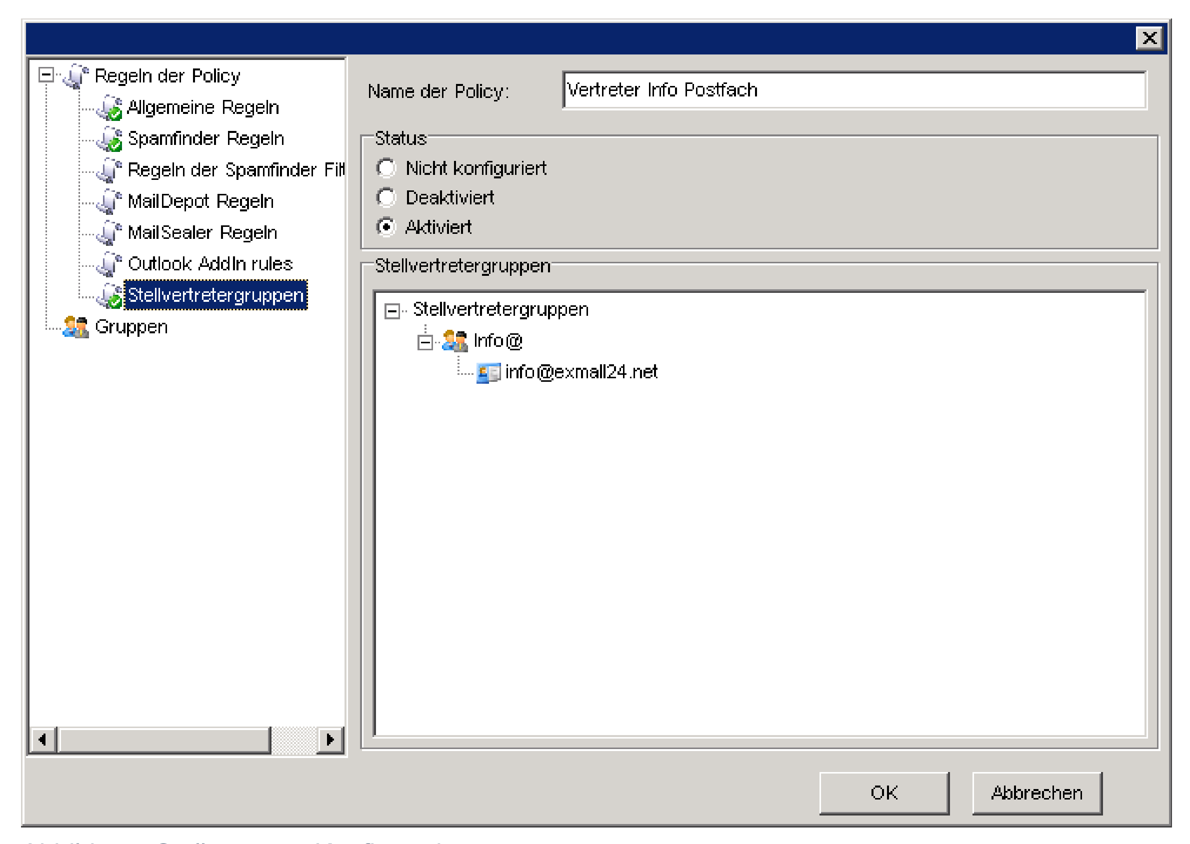



Abbildung: Stellvertreter-Konfiguration

1. Klicken Sie rechts auf Stellvertreter-Gruppen.
2. Wählen Sie *Hinzufügen einer Stellvertretergruppe* aus.
3. Geben Sie der neuen Stellvertretergruppe einen Namen.
   Mit rechtem Mausklick auf die neue Stellvertretergruppe können Sie:
   3.1 Die Stellvertretergruppe wieder *löschen.*
   3.2 Die Stellvertretergruppe *umbenennen*.
   3.3 Eine Stellvertreter-E-Mail-Adresse hinzufügen.
      Durch Rechtsklick auf die E-Mail-Adresse kann diese wieder aus der Gruppe gelöscht werden.

**HINWEIS - AUSNAHME GEGENÜBER ANDEREN RULE-SETS**

Die Liste aller E-Mail-Adressen, die ein Benutzer vertreten darf, wird aus ALLEN Policies gebildet, deren Benutzer-Gruppe der Benutzer zugeordnet ist.

## 4.3.3 Benachrichtigung

**Informationen zu Benachrichtigungen**

Über die Benachrichtigungen können Sie die Standardtexte, der in der jeweiligen Situation versandten E-Mails bearbeiten.

**Folgende Standardtexte sind konfigurierbar:**

- CISS
- Adressüberprüfung
- Virusmeldung an Administrator
- Virusmeldung an Empfänger
- Virusmeldung an Absender

**CISS Benachrichtigung bearbeiten**

Bei der CISS Benachrichtigung können Sie die Sprache, den Betreff und den Inhalt der E-Mail anpassen.

**Einschränkung:** Keine.

1. Wählen Sie in der Baumansicht ***Benachrichtigungen*** aus.
2. Klicken Sie in der Listenansicht mit der rechten Maustaste auf 'CISS'.
3. Wählen Sie in der Auswahlliste den Eintrag **Bearbeiten**.
   Folgende Felder werden angezeigt:

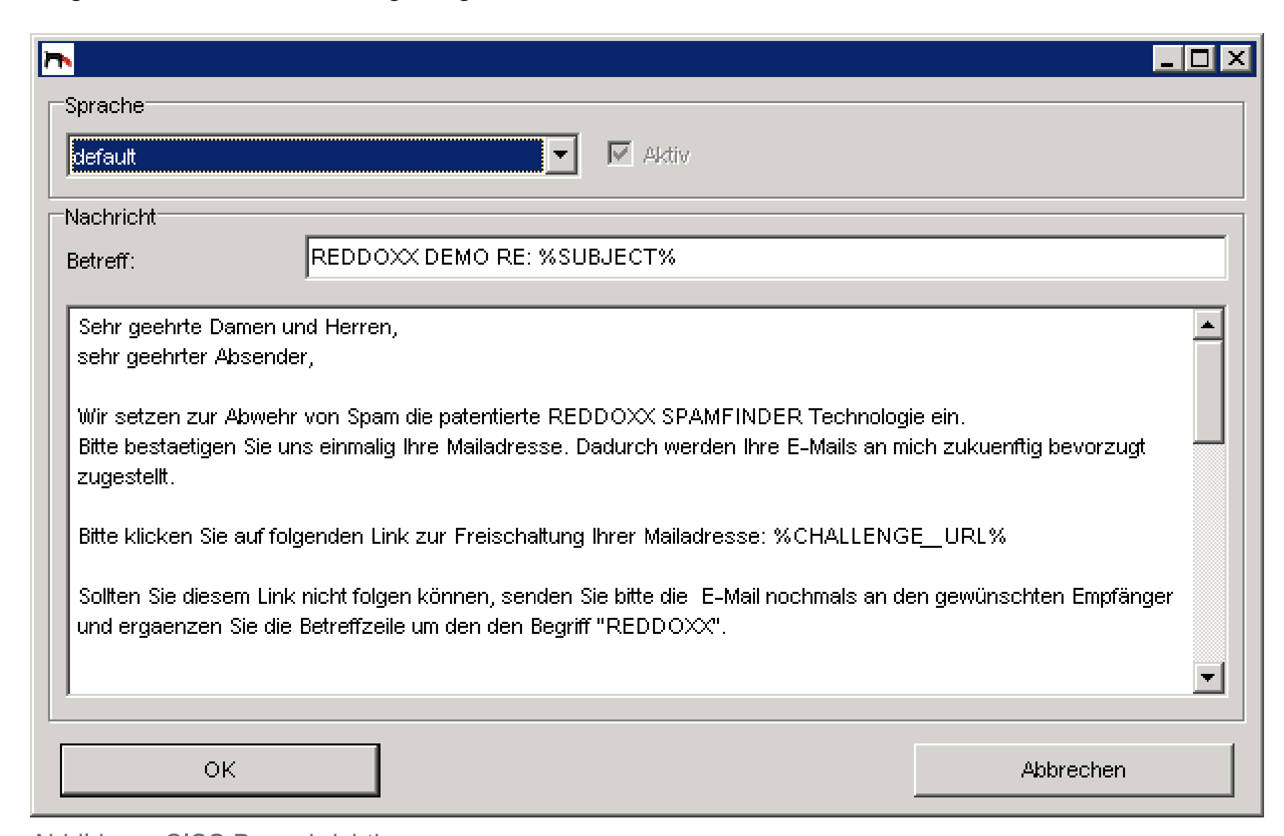



Abbildung: CISS Benachrichtigung

4. Wählen Sie über die Auswahlliste die gewünschte Sprache aus.
   Die Standardeinstellung beinhaltet den Text der E-Mail in Deutsch und Englisch.
5. Aktivieren Sie die Option *Feld*, um die Sprache zu aktivieren.
6. Ändern Sie die E-Mail nach Ihren Vorstellungen.

**HINWEIS**

Die in Prozentzeichen gefassten Texte stellen Platzhalter dar und dürfen weder geändert noch gelöscht werden.

7. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Platzhalter der CISS Benachrichtigung:**

| PLATZHALTER | ERKLÄRUNG |
|---|---|
| %SUBJECT% | Betreff der empfangenen E-Mail |
| %CHALLENGE_URL% | URL zum REDDOXX Portal |

**Benachrichtigung für Adressüberprüfung bearbeiten**

Bei der Benachrichtigung für die Adressüberprüfung können Sie den Betreff und den Inhalt der E-Mail anpassen.

**Einschränkung:** Keine.

1. Wählen Sie in der Baumansicht ***Benachrichtigungen*** aus.
2. Klicken Sie in der Listenansicht mit der rechten Maustaste auf 'Adressüberprüfung'.
3. Wählen Sie in der Auswahlliste den Eintrag **Bearbeiten**.
   Folgende Felder werden angezeigt:

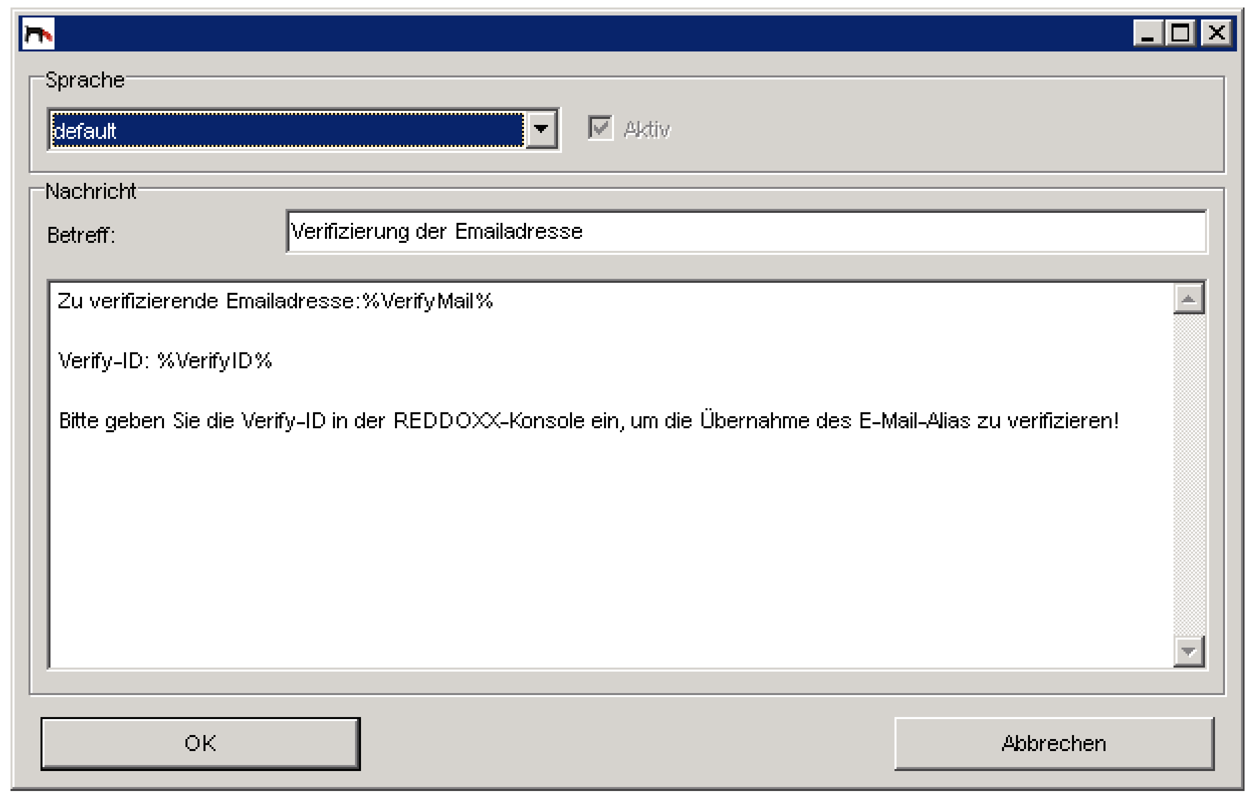



Abbildung: Benachrichtigung für Adressüberprüfung

4. Ändern Sie die E-Mail nach Ihren Vorstellungen.

**HINWEIS**

Die in Prozentzeichen gefassten Texte stellen Platzhalter dar und dürfen weder geändert noch gelöscht werden.

5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Platzhalter der Benachrichtigung für Adressüberprüfung:**

| PLATZHALTER | ERKLÄRUNG |
|---|---|
| %VerifyMail% | zu prüfende E-Mail-Adresse |
| %VerifyID% | ID (Nummer) die zur Bestätigung der E-Mail-Adresse eingegeben werden muss |

**Benachrichtigung bei Virenmeldung bearbeiten**

Bei der Benachrichtigung für die Virenmeldung können Sie den Betreff und den Inhalt der E-Mail anpassen. Diese Benachrichtigungen können an den Administrator, den Empfänger und den Absender verfassen.

**Einschränkung:** Keine.

1. Wählen Sie in der Baumansicht ***Benachrichtigungen*** aus.
2. Klicken Sie in der Listenansicht mit der rechten Maustaste auf 'Virenmeldung an Administrator'.
3. Wählen Sie in der Auswahlliste den Eintrag **Bearbeiten**.
   Folgende Felder werden angezeigt:

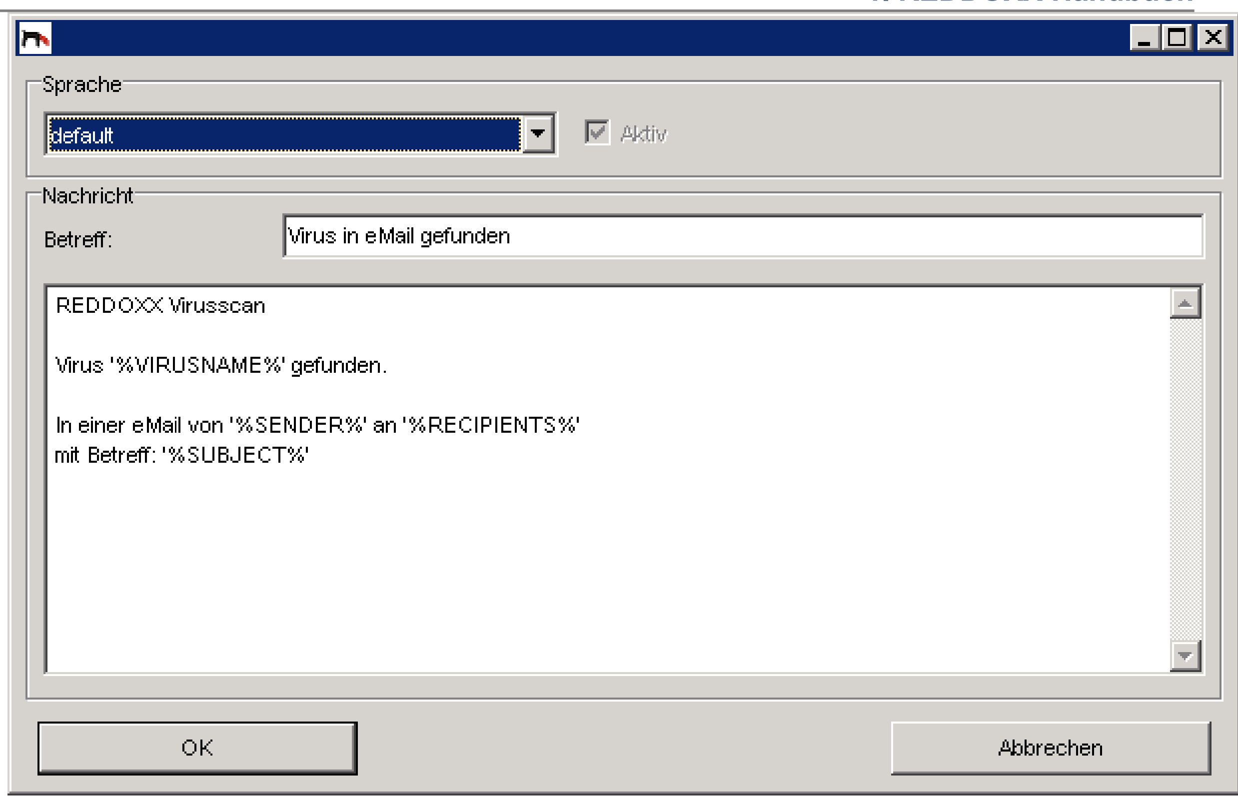



Abbildung: Benachrichtigung bei Virenmeldung an den Administrator

4. Ändern Sie die E-Mail nach Ihren Vorstellungen.

**HINWEIS**

Die in Prozentzeichen gefassten Texte stellen Platzhalter dar und dürfen weder geändert noch gelöscht werden.

5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**HINWEIS**

Gehen Sie für die Virenmeldung an den Empfänger und den Absender gleich vor.

**Platzhalter der Benachrichtigung bei Virenmeldung:**

| PLATZHALTER | ERKLÄRUNG |
|---|---|
| %VIRUSNAME% | Name des gefundenen Virus |
| %SENDER% | Absender der E-Mail |
| %RECIPIENTS% | Empfänger der E-Mail |
| %SUBJECT% | Betreff der E-Mail |

## 4.3.4 Protokolle

Die REDDOXX Appliance erstellt für jeden Tag eine Protokolldatei. Diese werden in der Listenansicht aus dem Menübaum *Protokolle* dargestellt. Sie haben folgendes Dateinamensformat:

Appliance-yyyy-mm-dd_HH:MM.log, wobei *yyyy=Jahr, mm=Monat, dd=Tag, HH=Stunde, MM=Minute* bedeutet.
Übersteigt das Protokoll die Dateigröße von 50 MB, so wird eine neue Protokolldatei mit aktuellem Zeitstempel erzeugt.

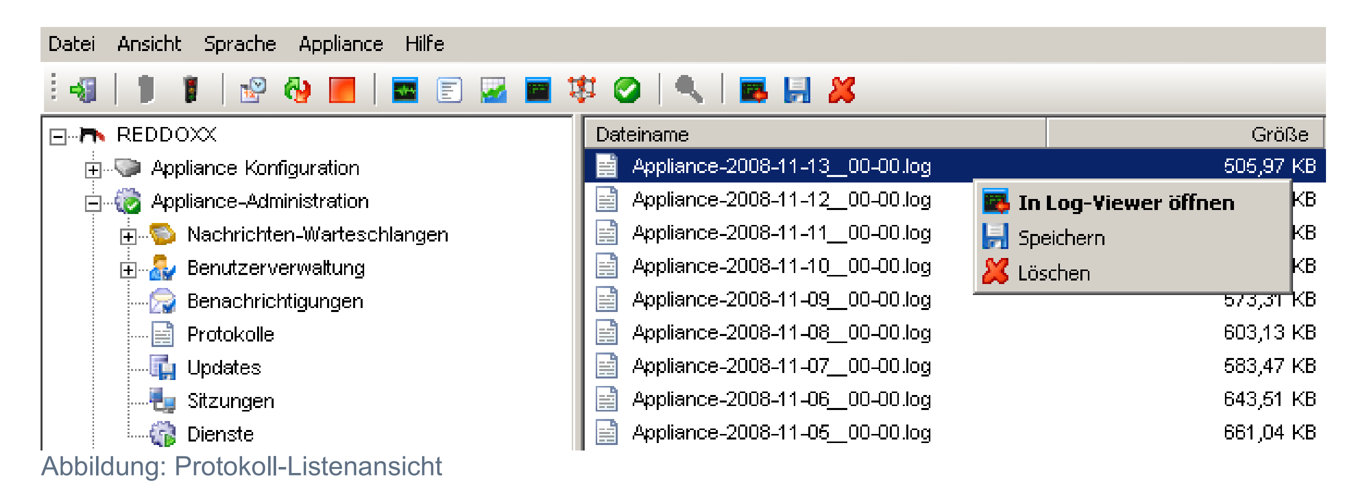


Abbildung: Protokoll-Listenansicht

Die Protokolle können durch eine spezielle Protokollanalyse (Log Viewer) angezeigt und ausgewertet werden.
Es gibt folgende Möglichkeiten Protokolle zu analysieren:

- Gesamtes Protokoll im Log Viewer
- Filter nach Prozess ID
- Smart Filter
- Protokoll in lokales System speichern

**Gesamtes Protokoll**

Um das Protokoll eines bestimmten Tages mit dem Log Viewer anzuschauen, klicken Sie in der Baumansicht  auf Protokolle und doppelklicken das gewünschte Protokoll aus der Liste. Es erscheint folgender Ansicht:

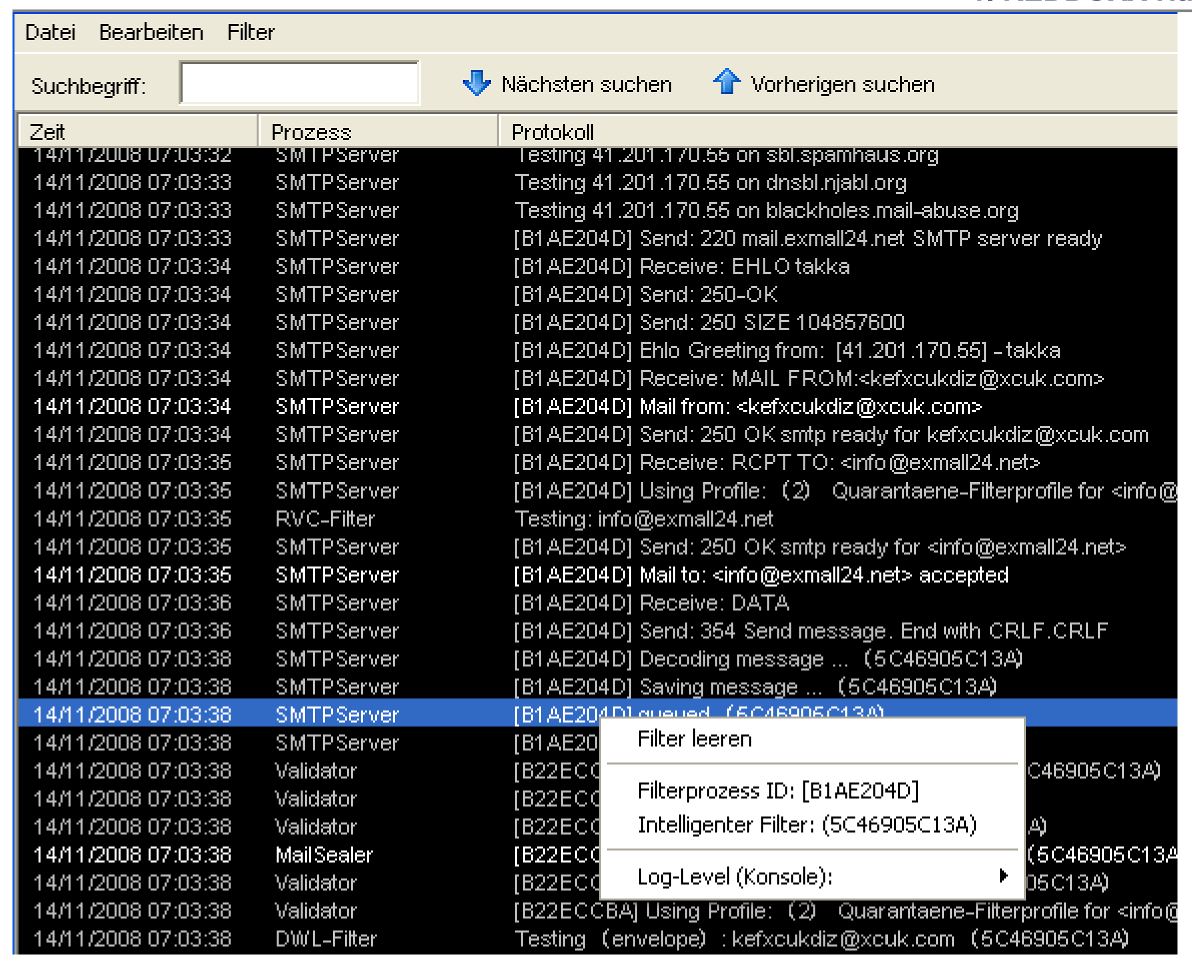



Abbildung: Protokollansicht

**ProzessID**

Es gibt die Möglichkeit, die Log-Informationen eines bestimmten Prozesses zu filtern. Dazu muss im Log Viewer eine bestimmte Prozess ID gewählt werden. Die Prozess ID kann an den eckigen Klammern erkannt werden. So kann z.B. der gesamte Empfangs-Protokolldialog einer Mail durch Filtern der Prozess ID 3045965838, wie in der Abbildung zu sehen, detailliert dargestellt werden.

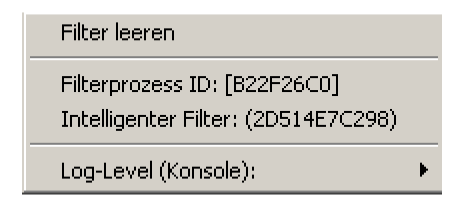
**Smart Filter**

Da es öfters erwünscht ist, den Verlauf einer zusammengehörigen Aktion zu filtern z.B. den Mailfluss einer E-Mail, dieser aber verschiedene Prozesse durchläuft, kann anhand der Smart ID, oder auch Message ID genannt, der Verlauf gefiltert werden. Die Smart ID ist in runden Klammern zu finden.

**Funktionsweise der Filterung (Prozess/Smart)**

1. Klicken Sie im Log Viewer auf eine gewünschte ID (Smart oder Prozess ID) mit der rechten Maustaste.

2. Es erscheint folgendes Menü:




3. Wählen Sie die gewünschte Filterart.
4. Der Log Viewer zeigt nur noch die entsprechenden Daten an.
5. Um das Filtern aufzuheben, kann mit einem weitern Rechtsklick über die Option Filter löschen das Filtern aufgehoben werden.

#### 4.3.4.1 Filterfunktion in der Echtzeit-Protokollanzeige

Ab der Version 1025 ist es möglich, das Live-Log (Echtzeit-Protokollanzeige) zu filtern. Klicken Sie in der Protokollierungsanzeige mit der rechten Maustaste auf einen Protokolleintrag. Es erscheint das Kontextmenü, wie nachfolgend angezeigt.

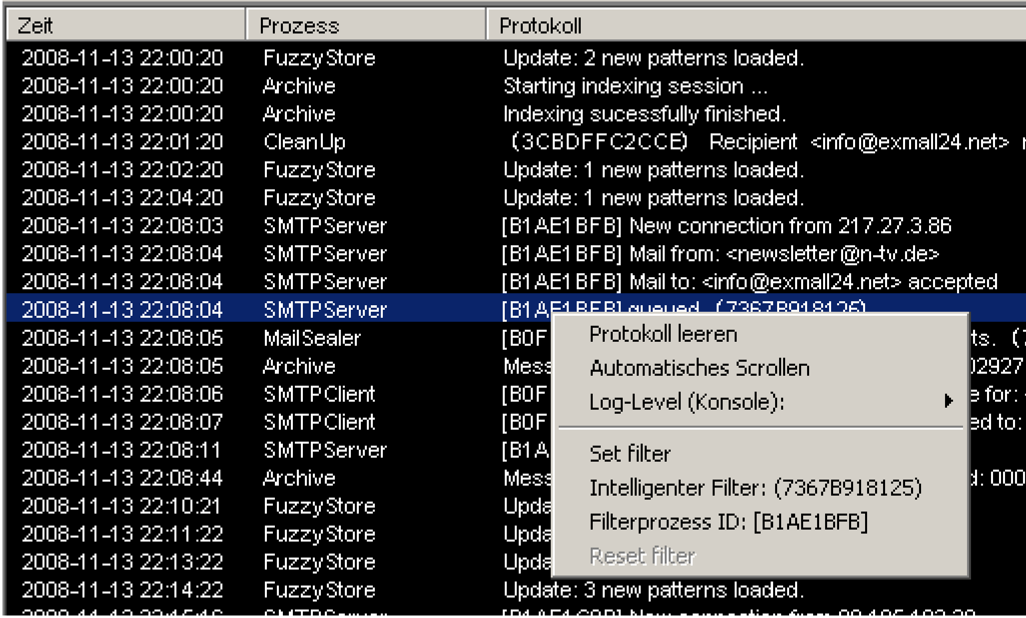



Abbildung: Echtzeit-Protokollanzeige mit Filtereigenschaften

**Set filter**

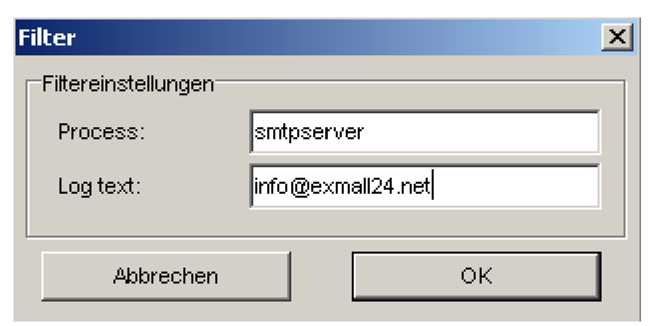



Abbildung: Echtzeit-Protokollanzeige mit Filtereigenschaften

**Process:**
Geben Sie hier einen Prozess-Typ ein, nachdem gefiltert werden soll.

**HINWEIS**

Mögliche Prozess-Typen sind:

*ABL-Filter, AWL-Filter, Advanced-RBL-Filter, AntiSpoofing, Archive, AutoWLAdjustment, Backup, Bayes, Bayes-Filter, BounceMail, CISS, CleanUp, Cleanup, ControlServer, DBL-Filter, DWL-Filter, Fuzzy-Filter, FuzzyStore, RBL-Filter, RVC-Filter, Report, SBL-Filter, SMTPClient, SMTPServer, SRC-Filter, SWL-Filter, SendMail, Stats, System, Validator, VirusScanner, permanently*

Die Angabe ist case-insensitive, d.h. es wird nicht zwischen Groß- und Kleinschreibung unterschieden.

**Log text:**
Geben Sie hier den Text ein, nachdem Sie in der Spalte „Protokoll" suchen möchten.

**Intelligenter Filter:**
wie beim Logviewer.

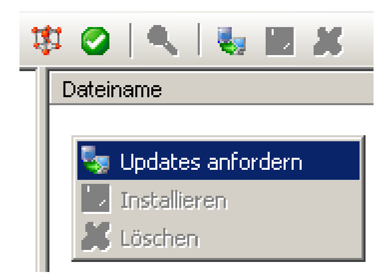
**Filterprozess ID:**
wie beim Logviewer.

### 4.3.5 Updates

**Updates anfordern**

Das Erscheinen neuer Updates erfahren Sie durch die Release Notes. Diese senden wir Ihnen per E-Mail auf die in den EINSTELLUNGEN angegebener Admin-Adresse zu. Das Update fordern Sie selbst folgendermaßen an.
**Voraussetzungen:** Eine gültige Subscription-Lizenz.

1. Wählen Sie in der Baumansicht ***Updates*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
   Folgende Ansicht wird angezeigt:




**HINWEIS**

Sollte die Option „UPDATES ANFORDERN" nicht erscheinen, so benutzen Sie noch eine alte Konsolensoftware. Laden Sie sich dann die neuste Konsolensoftware herunter und benutzen Sie diese, um das Update erneut anzufordern.

3. Wählen Sie den Eintrag **Updates anfordern**
   Folgende Ansicht wird angezeigt:




Das Update sollte, je nach Bandbreite, nach wenigen Sekunden bis Minuten in der Listenansicht erscheinen. Sie können die Listenansicht durch Drücken der F5-Taste aktualisieren. Nach Beendigung des Downloads erscheint rechts unten folgende Anzeige:




**HINWEIS**

Der Anti-Virenschutz und Antispam-Filter wird automatisch aktualisiert! Überprüfen Sie, ob ausreichend gültige Lizenzen vorhanden sind. Die AV-Version sollte nicht älter als 1-2 Tage sein.

### Updates installieren

Über den Menüpunkt Updates können Sie aktuelle Updates installieren.

**Voraussetzungen:** Updates in der Liste vorhanden.

1. Wählen Sie in der Baumansicht ***Updates*** aus.
2. Wählen Sie das gewünschte Update aus und klicken Sie in der Listenansicht die rechte Maustaste.




Abbildung: Auswahl eines Updates zur Installation

3. Wählen Sie in der Auswahlliste den Eintrag **Installieren**.
   Es erscheint folgender Dialog:

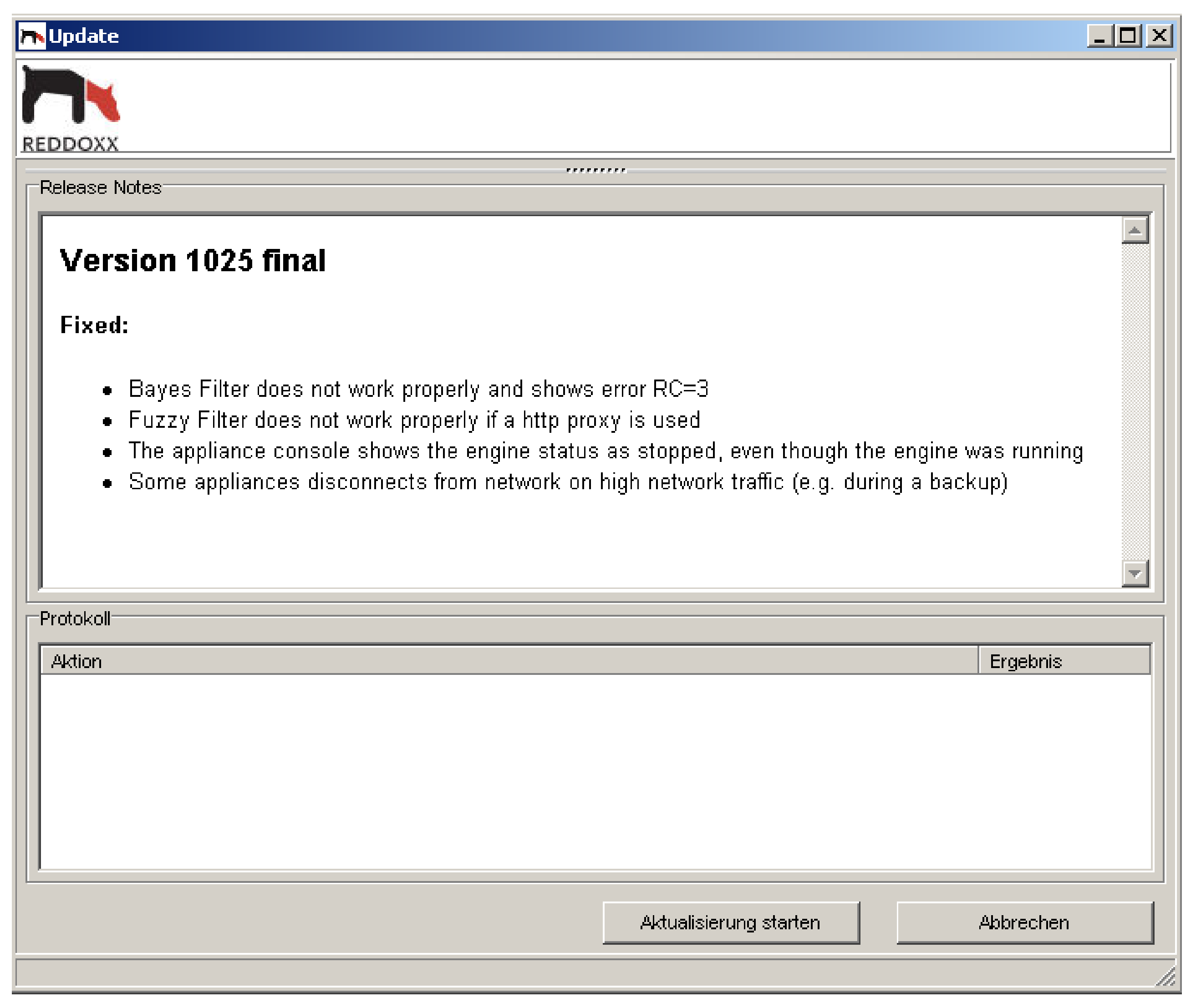



Abbildung: Auswahl eines Updates zur Installation

4. Im oberen Fensterbereich werden die Release Note angezeigt. Bitte lesen Sie sich diese aufmerksam durch.
5. Klicken Sie auf ***Aktualisierung starten***, um das Update zu installieren.
   Danach startet das Update und die neue Firmware wird eingespielt. Dies dauert i.d.R. nur wenige Minuten. Während des Updates können Sie die einzelnen Schritte im Protokollfenster verfolgen.

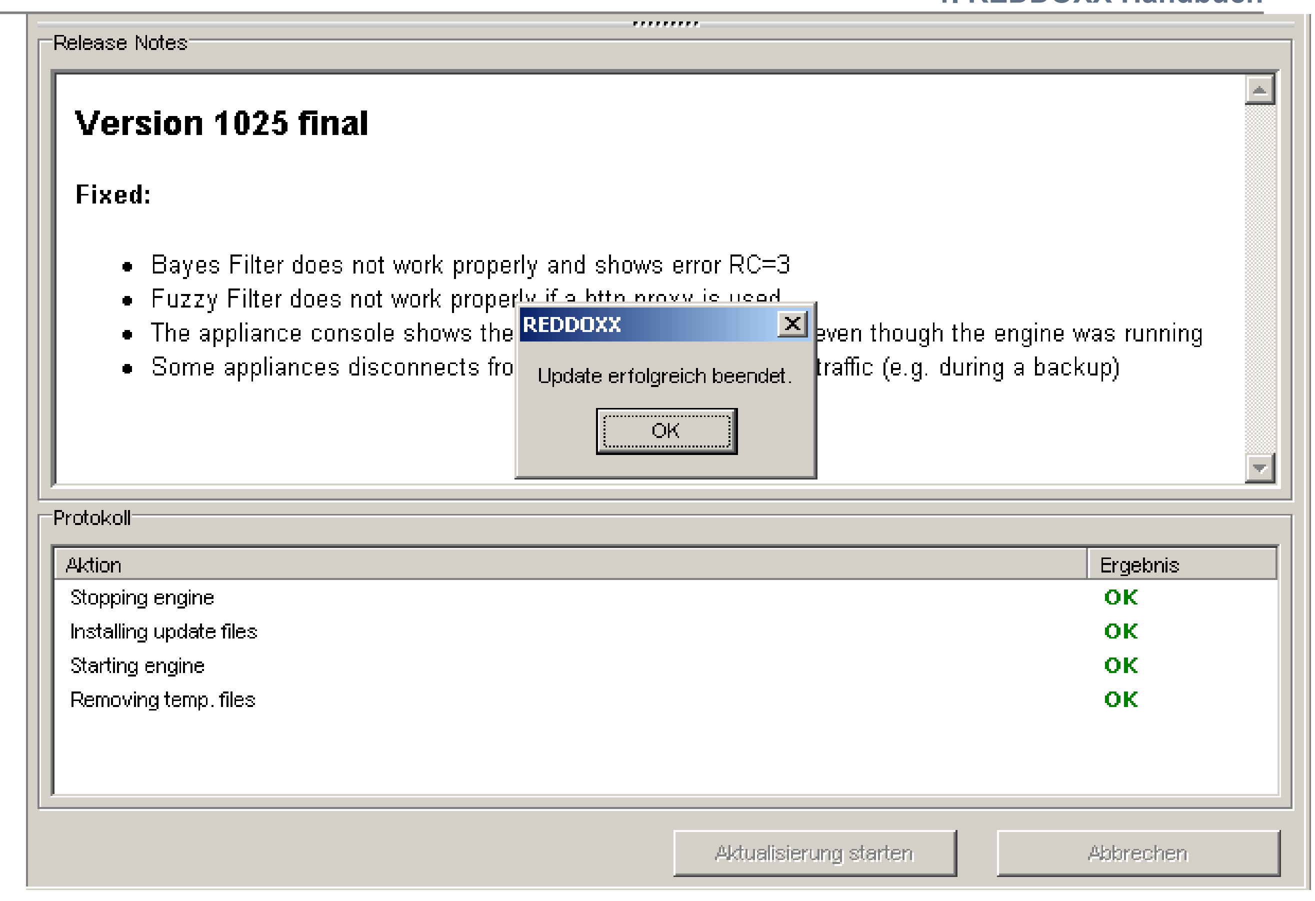
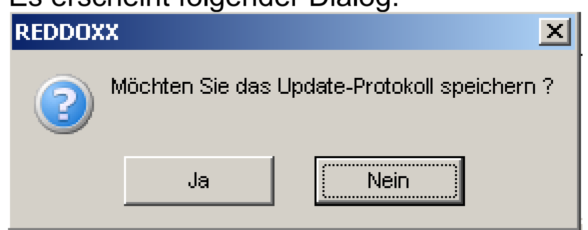



Abbildung: Protokollansicht eines Firmware-Updates.

6. Nach Beendigung erscheint ein Nachrichtendialog, den Sie mit OK bestätigen. Ein Reboot der Appliance ist in den meisten Fällen nicht mehr erforderlich. Damit die Änderungen aber wirksam werden, startet die Appliance-Engine selbständig neu. Dabei bricht zwar die Verbindung mit der Adminkonsole kurzzeitig ab, aber die Konsole verbindet sich nach wenigen Sekunden wieder erneut von selbst.
7. Klicken Sie auf OK um das Updateprotokollfenster zu schließen.
   Es erscheint folgender Dialog:




8. Wurde beim Update ein Fehler angezeigt, speichern und prüfen Sie das Update-Protokoll und schauen Sie im Support- FAQ-Bereich nach möglichen Lösungen. (http://support.reddoxx.net). Nehmen Sie geg.falls Kontakt mit dem Reddoxx-Support auf und geben Sie das Protokoll mit an.

**HINWEIS**

Updates müssen in der Versions-Reihenfolge nacheinander installiert werden.
Release Notes immer aufmerksam durchlesen.

Beachten Sie auch, dass bei Software-Updates nur die aktive Appliance upgedated werden muss. Das Update wird im Clusterbetrieb automatisch auf dem passiven Knoten installiert.

**Updates löschen**

Normalerweise wird das Update nach dem Installieren durch die Appliance gelöscht. Sie können aber auch manuell das Update löschen.

### 4.3.6 Sitzungen

**Informationen zu Sitzungen**

Über die ***Sitzungen*** können Sie alle an der REDDOXX Appliance angemeldeten Benutzer einsehen.

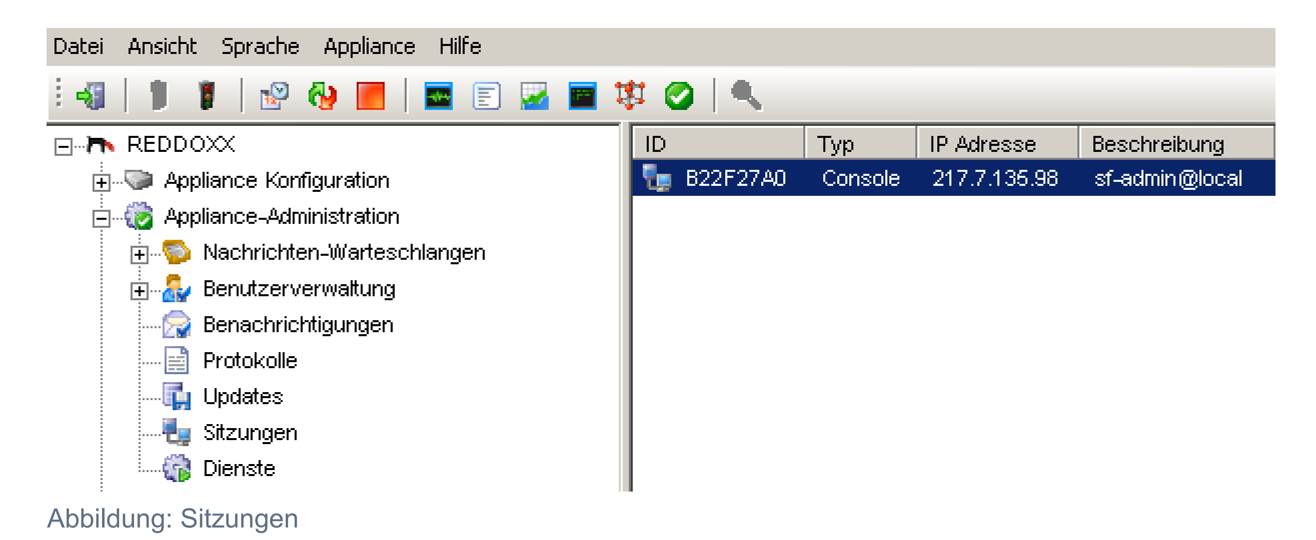



Abbildung: Sitzungen

### 4.3.7 Dienste

#### 4.3.7.1 Überblick

Über die Diensteverwaltung können Sie einzelne Dienste einsehen und steuern.

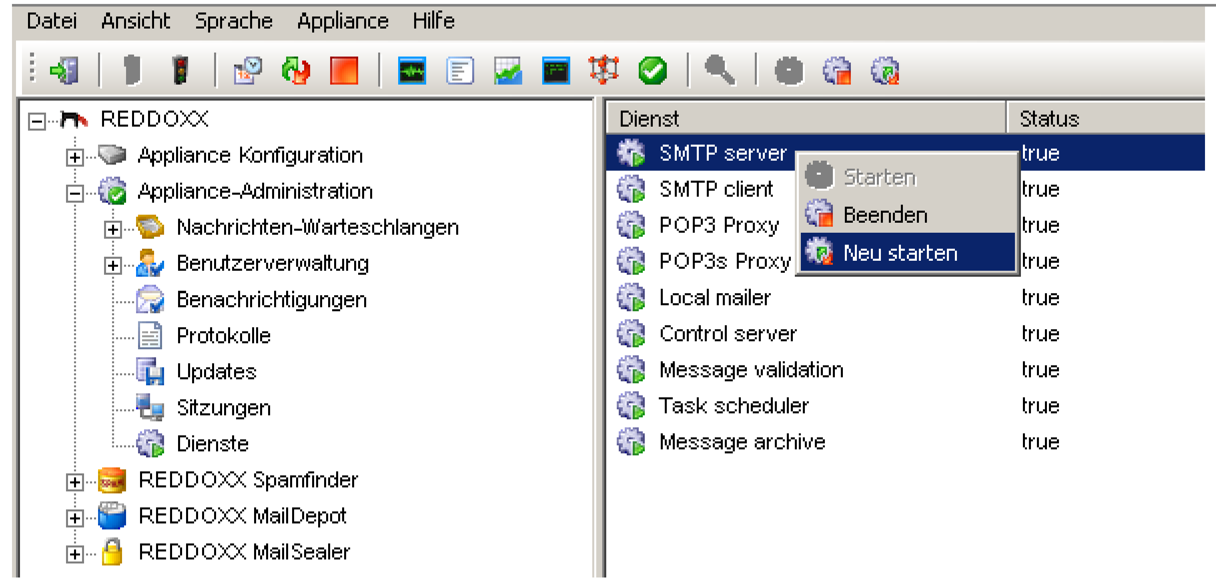



Abbildung: Dienste

### 4.3.7.2 Mail-Fluss

Nachfolgende Skizze zeigt den Mailfluss einer E-Mail:
Mailannahme (SMTP-Server) → Überprüfung (Validator) → Zustellung (SMTP-Client)

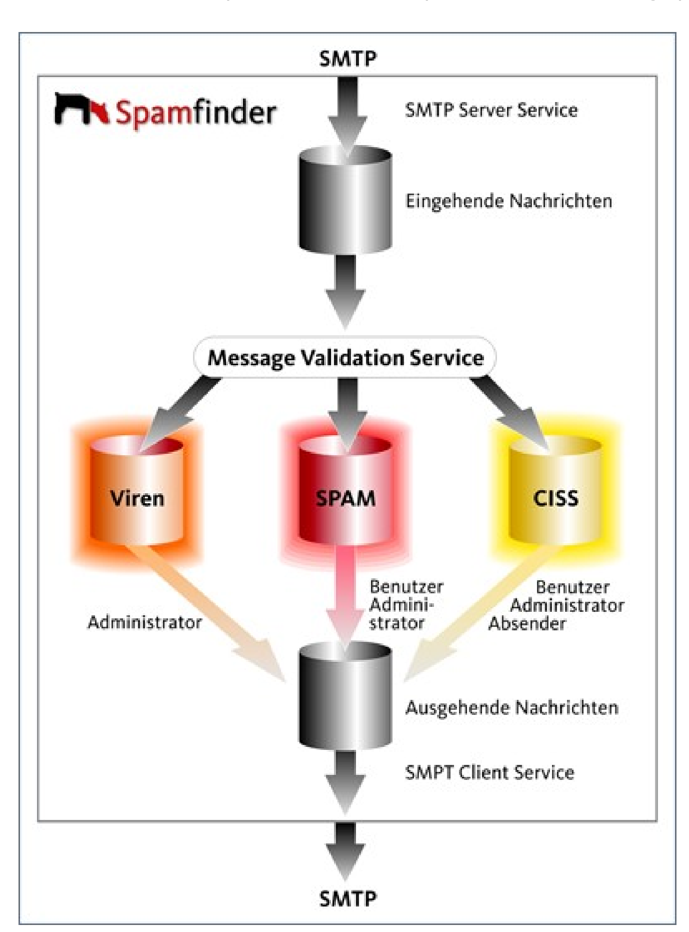



Abbildung: Schema Mailfluss

#### 4.3.7.3 SMTP Server Service

Der SMTP Server nimmt E-Mails von anderen E-Mail-Servern entgegen und speichert die E-Mails in der Warteschlange *"Eingehende Nachrichten".* Bevor die E-Mails entgegen genommen werden, werden die Filter der Phase 1 überprüft.

#### 4.3.7.4 SMTP Client Service

Der SMTP Client Service versendet E-Mails, die in der Warteschlange *"Ausgehende Nachrichten"* auf den Versand warten.

#### 4.3.7.5 Control Server Service

Der Control Server bedient die Verbindungen der Administrator-Konsolen sowie der Benutzer-Konsole und dient zur Konfiguration und Verwaltung der REDDOXX Appliance.

#### 4.3.7.6 Message Validation Service

Der Message Validation Service überprüft alle E-Mails aus der Warteschlange *"Eingehende Nachrichten".* Dabei werden die E-Mails durch die Filter aus der Phase 2 geprüft und auf Viren untersucht. Abhängig vom Ergebnis der Prüfung werden die E-Mails dann in eine der folgenden Warteschlangen verschoben: Viren, Spam oder CISS.

#### 4.3.7.7 Task Scheduler Service

Der Task Scheduler Service startet zyklisch Prozesse, wie zum Beispiel das Aufräumen der Warteschlangen und das Update von Viren- und Spam-Signaturen.

#### 4.3.7.8 Portal Communication Service

Der Portal Communication Service verarbeitet E-Mails die vom REDDOXX Portal versendet wurden, zum Beispiel CISS. Er sorgt durch verschlüsseln beziehungsweise entschlüsseln der E-Mails für eine sichere Kommunikation mit dem REDDOXX Portal.

#### 4.3.7.9 Remote Support Service

Der REDDOXX Remote Support Service ermöglicht dem REDDOXX Support eine verbesserte Fernwartung ohne dass Regel-Änderungen an Ihrer Firewall nötig sind. Der REDDOXX Remote Support Service ist immer deaktiviert, und sollte nur nach Rücksprache mit einem REDDOXX-Supportmitarbeiter gestartet werden. Bei aktiviertem Support Service wird eine Verbindung ausgehend zu unserem Vermittlungsrechner aufgebaut, über den sich die Mitarbeiter des technischen Supports von REDDOXX dann auf Ihre Appliance aufschalten können, um weitere Diagnosen durchzuführen.

#### 4.3.7.10 Dienste starten, beenden und neustarten

**Dienst starten**

Über die Dienste können Sie einen nicht laufenden Dienst starten.
**Voraussetzungen:** Aktueller Status 'false'.

1. Wählen Sie in der Baumansicht ***Dienste*** aus.
2. Klicken Sie den zu startenden Dienst mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Starten**.



**Dienst beenden**

Über die Dienste können Sie einen laufenden Dienst beenden.
**Voraussetzungen:** Aktueller Status 'true'.

1. Wählen Sie in der Baumansicht ***Dienste*** aus.
2. Klicken Sie den zu beendenden Dienst mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Beenden**.




**Dienst neu starten**

Über die Dienste können Sie einen laufenden Dienst neu starten.
**Voraussetzungen:** Aktueller Status 'true'.

1. Wählen Sie in der Baumansicht ***Dienste*** aus.
2. Klicken Sie den Dienst, den Sie neu starten möchten, mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu starten**.




## 4.4 REDDOXX Spamfinder

Im Bereich Spamfinder werden Einstellungen zur Verwaltung von Filtereinstellungen und der Spamwarteschlangen vorgenommen.

### 4.4.1 Spamfinder-Warteschlangen

E-Mails, die noch nicht zugestellt wurden, finden Sie einer der folgenden Warteschlangen. Für alle Warteschlangen gilt, dass Sie eine dort gelistete E-Mail mit einem Rechtsklick zustellen oder löschen können. Zum Sortieren der Listeneinträge klicken Sie auf die gewünschte Spaltenüberschrift. Nochmaliges Klicken kehrt die Sortierung um. Der Inhalt einer E-Mail kann wegen gesetzesrechtlicher Bestimmungen nicht eingesehen werden. Bedenken Sie auch, dass E-Mails, die Sie hier nicht finden können, bereits in der Ausgabewarteschlange sind:

*Spam Warteschlange*

E-Mails die in der Spam Warteschlange gelistet sind, wurden von der REDDOXX Appliance als Spam klassifiziert. In der 7. Spalte "Filter" sehen Sie, welcher Antispam-Filter angeschlagen hat.

| ID | Erhalten am | Absender | Empfä... | Größe | Betreff | Filter |
|---|---|---|---|---|---|---|
| 1B06F96A924 | 23.04.200... | emailSender... | info@b... | 43,64 KB | Elektronik-Restposten ra... | Bayes-Filter |
| 26C84CE7474 | 23.04.200... | verdopiri@pa... | info@b... | 48,87 KB | Was meinst du, w?rde ... | RBL-Filter |
| 547CEA9B86C | 23.04.200... | sybillavalenk... | info@b... | 21,86 KB | Trinidad | RBL-Filter |
| 47FDE5C9A3D | 23.04.200... | sds@greent... | info@b... | 3,08 KB | FDA approved on-line p... | Fuzzy-Filter |
| 8A1A94DC2D | 23.04.200... | pytcongrexp... | info@b... | 5,12 KB | Less weight - more plea... | RBL-Filter |
| 3D8D012CCF7 | 23.04.200... | considerable... | info@b... | 2,75 KB | Lulu - 100% results. | RBL-Filter |
| 137DBDF0A10 | 23.04.200... | techdata-DK... | info@b... | 45,70 KB | Erinnerung: Achte Pow... | Bayes-Filter |

Abbildung: Spamwarteschlange

**HINWEIS**

Nur wenn der Filter die Aktion "QUARANTÄNE" eingestellt hat, wird die E-Mail in der Spam-Warteschlange gelistet.

### *CISS Warteschlange*

E-Mails, deren Absender dem Spamfinder noch unbekannt sind (==> noch nicht in der Address- oder Domain-Whitelist eingetragen), landen bei aktiviertem CISS-Filter in der CISS-Warteschlange.

**HINWEIS**

Achten Sie darauf, dass für die Filter AWL und DWL die ÜBERSTEUERUNG des Negativfilters CISS aktiviert ist. Weitere Details zur CISS-Filtertechnologie finden Sie im Kapitel 4.4.2.5 Filter - CISS.

### *Viren und verbotene Dateiendungen*

E-Mails mit Viren im Anhang, oder Anhänge mit nicht erlaubten Dateiendungen landen in der Viren-Warteschlange. Gezippte Dateiendungen werden ebenfalls auf Viren durchsucht, sofern Sie nicht verschlüsselt sind.

**HINWEIS**

Ausschließlich der Administrator kann die Viren-Warteschlange einsehen und verwalten.

Die Warteschlangen können durchsucht und Einträge gelöscht werden.
**Siehe auch:** "Appliance-Administration - Nachrichtenwarteschlangen".

### E-Mail zustellen

In den jeweiligen Warteschlangen können Sie E-Mails an den Empfänger zustellen.
**Einschränkung:** Zustellen der E-Mails nur in den Warteschlangen Spam, CISS und Viren möglich.

1. Wählen Sie in der Baumansicht ***Warteschlangen*** mit einem Doppelklick aus.
2. Wählen Sie die gewünschte Warteschlange aus.

3. Klicken Sie die zuzustellende E-Mail mit der rechten Maustaste an.
4. Wählen Sie in der Auswahlliste den Eintrag **Zustellen**.

**E-Mail zustellen (Whitelist)**

In den jeweiligen Warteschlangen können Sie E-Mails an den Empfänger zustellen und diesen gleichzeitig in die Whitelist eintragen lassen.

**Einschränkung:** Zustellen der E-Mails nur in den Warteschlangen Spam und CISS möglich.

1. Wählen Sie in der Baumansicht ***Warteschlangen*** mit einem Doppelklick aus.
2. Wählen Sie die gewünschte Warteschlange aus.
3. Klicken Sie die zuzustellende E-Mail mit der rechten Maustaste an.
4. Wählen Sie in der Auswahlliste den Eintrag **Zustellen (Whitelist)**.

**E-Mails sortieren**

In den jeweiligen Warteschlangen können Sie E-Mails über den Spaltenkopf in der Listenansicht sortieren.

**Voraussetzung:** E-Mails in den Warteschlangen vorhanden.

1. Wählen Sie in der Baumansicht ***Warteschlangen*** mit einem Doppelklick aus.
2. Wählen Sie die gewünschte Warteschlange aus.
3. Klicken Sie die doppelt auf den Spaltenkopf, nach dem Sie Ihre E-Mails sortieren möchten.
   Die Sortierung erfolgt alphabetisch.

## 4.4.2 Filter

**Informationen zu Filtern**

Im Gegensatz zur Konzentration auf das, was man nicht erhalten möchte, filtert die REDDOXX Appliance die E-Mails heraus, die der Benutzer erhalten möchte.
Deshalb basiert die Technologie auf den modernsten und innovativsten Filtertechniken.
Die Folge der verschiedenen Filtertechnologien kann individuell konfiguriert und über verschiedene Profile den Benutzern auch individuell zur Verfügung gestellt werden.

**Wie E-Mails gefiltert werden**

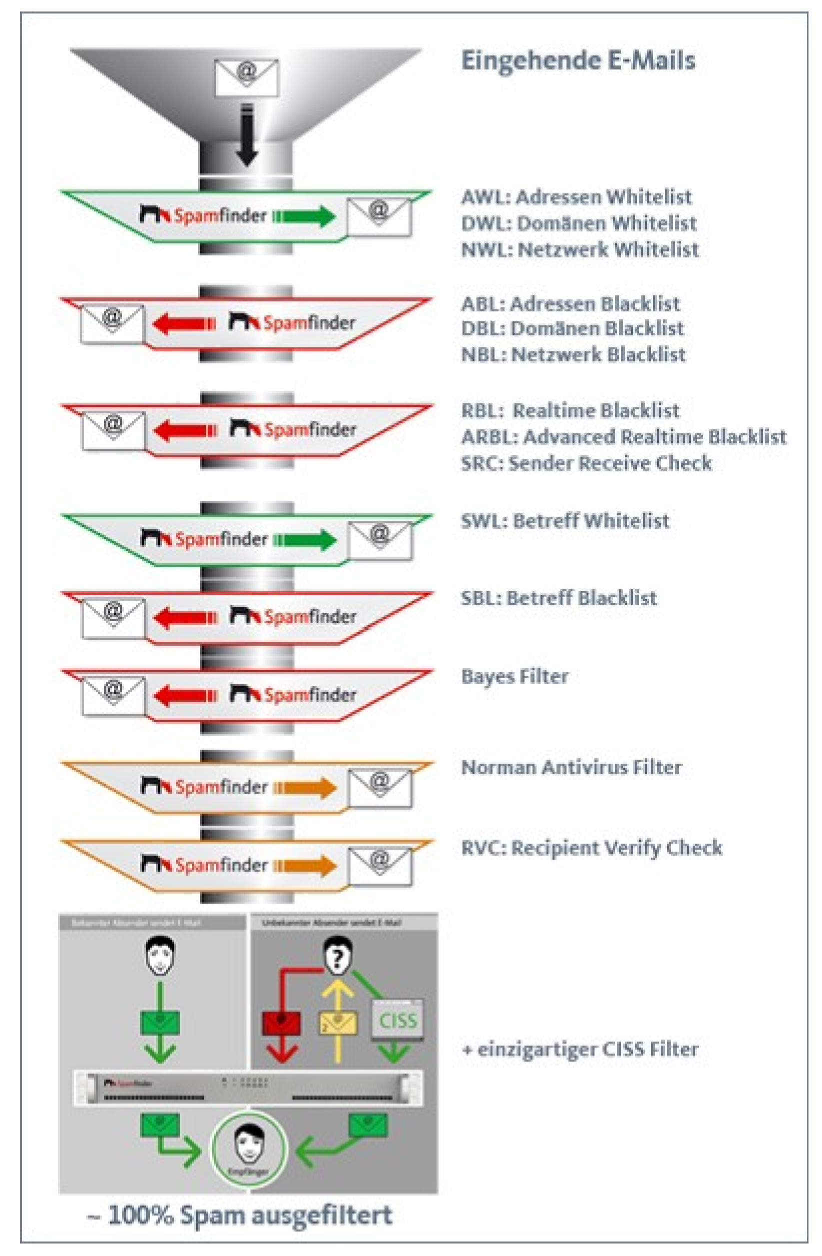



Abbildung: Filterschema

#### 4.4.2.1 Whitelist Filter

Whitelists sind so genannte freundliche Listen und sofern bestimmte Kriterien erfüllt sind, werden die E-Mails ohne weitere Verzögerung direkt zugestellt. Diese Listen variieren von individuellen E-Mail-Adressen bis hin zu allgemeinen Domänenadressen. Sie können einzelne IP-Adressen oder IP-Adressbereiche beinhalten oder einfach nur bestimmte Betreffinhalte, die eine E-Mail als "erwünscht" klassifizieren. Beim der REDDOXX Spamfinder wurden diese Listen wie folgt implementiert:

- AWL: Adressen Whitelist
- DWL: Domänen Whitelist
- NWL: Netzwerk Whitelist
- SWL: Betreff Whitelist

Diese Filterlisten gibt es auf einer allgemeinen Basis für alle Benutzer eines Systems, aber auch für jeden einzelnen Benutzer, um die Treffsicherheit des REDDOXX Spamfinders zu perfektionieren.

**Whitelist Auto-Add Adjustment**

Die Whitelisten werden automatisch ergänzt, sobald ein Benutzer eine E-Mail versendet. Dies geschieht, damit Antworten auf diese E-Mails als "erwünscht" angesehen und somit durchgestellt werden.

**HINWEIS**

Für die Auto Whitelist-Funktion ist es erforderlich, dass auch der ausgehende Mailverkehr über die REDDOXX Appliance geleitet wird

#### 4.4.2.2 Blacklist Filter

E-Mails von bestimmten Domänen, IP-Bereichen, E-Mail-Adressen oder mit bestimmten Betreffinhalten können durch die integrierten Blacklist-Technologien herausgefiltert werden. Diese Listen können vom Administrator unternehmensweit und zusätzlich vom Benutzer individuell erstellt und gepflegt werden.
Die Blacklist Filter des REDDOXX Spamfinders basieren aber auch auf externen, öffentlichen Listen. Ein allgemeines Problem dieser Filtertechniken ist das Risiko der Fehldetektion (so genannte False-Positives).
Die integrierte Benutzer-Quarantäne-Funktion des REDDOXX Spamfinders vermindert das Risiko der False-Positives, da jeder Benutzer die Möglichkeit hat, auf seinen Quarantänebereich zuzugreifen und sicherzustellen, dass keine E-Mail fälschlicherweise aussortiert wurde.
Auf diese Weise haben Administratoren auch einen geringen Aufwand, Spam auf der Suche nach wichtigen E-Mails zu durchsuchen.

**Die im REDDOXX Spamfinder integrierten Blacklist Filter sind:**

- ABL (Adressen Blacklist):
  Prüfung der Absenderadresse gegen eine im REDDOXX Spamfinder geführte Adress-Blacklist
- DBL (Domänen Blacklist):
  Prüfung der Absenderdomain gegen eine im REDDOXX Spamfinder geführte Domain-Blacklist.
- NBL (Netzwerk Blacklist):
  Prüfung der IP-Adresse eines absendenden E-Mailservers gegen eine im REDDOXX Spamfinder geführte Network-Blacklist.

- SBL (Betreff Blacklist):
  Prüfung der E-Mail-Betreffzeile (Subject) gegen eine im REDDOXX Spamfinder geführte Subject-Blacklist.

**Auf Basis von externen Servern gibt es folgende Filter:**

- RBL (Realtime Blacklist):
  Realtime Prüfung des sendenden E-Mailservers gegen öffentliche Blacklistserver.
- ARBL (Advanced Realtime Blacklist):
  Der Advanced Realtime Blacklist Filter prüft den letzten Mailserver innerhalb des Mailflusses, also denjenigen, der die E-Mail dem Spamfinder zustellt. Falls Sie Ihre E-Mails über ein eigenes Relay beziehen, muss dieses in der Konfiguration ausgeschlossen werden.
- Fuzzy Filter:
  Von REDDOXX entwickelter Filter, der den Inhalt der E-Mail mit bereits identifizierten Spammails vergleicht.
- SRC (Sender Receive Check):
  Der Sender Receive Check Filter wird benutzt, um festzustellen, ob eine E-Mail von einem existierenden E-Mail-Account aus versendet wurde. Dieser E-Mail-Account würde im Gegenzug eine Antwort seine E-Mail annehmen. Falls nicht, schlägt der SRC-Filter an. Damit E-Mails ohne gültigen Absender, wie zum Beispiel bei manchen Newsletter- oder Bestell-Systemen, versehentlich nicht zugestellt werden, empfehlen wir, die Filteraktion beim SRC auf MARKIEREN einzustellen. Zusätzlich können Sie Ihre gewünschten Newsletter-E-Mails in den White-Listen pflegen.

### 4.4.2.3 Inhaltsfilter

**SWL: Betreff Whitelist, SBL: Betreff Blacklist und Bayes Filter**

Inhaltsfilter, wie der Bayes Filter, sind auf jeden Benutzer angepasst und passen sich den Veränderungen von Spam an. Um E-Mails als Spam zu erkennen, verwenden diese Filter bayesische Checksummen, um die Wörter und Sätze einer E-Mail im Zusammenhang mit Ihrer Häufigkeit auf eine Spam-Wahrscheinlichkeit hin zu überprüfen. Zum Vergleich dienen vorangehende E-Mails (Spam und erwünschte E-Mails). Die Architektur der REDDOXX Spamfinder Inhaltsfilter nimmt Bezug auf das "CISS"-Verfahren, welche die Informationen der Inhaltsfilter erst in die Datenbank übernimmt, wenn das CISS erfolgreich bestanden wurde.

### 4.4.2.4 Globale Filter

**Antivirus Filter**

Als umfassendes Sicherheitssystem für E-Mails, beinhaltet die REDDOXX Appliance auch einen integrierten Virenschutz für Ihren E-Mail-Server. Um die hohen Qualitätsstandards der Filter zu unterstreichen, wird hier der Virenschutz der Open Source Software von ClamAV verwendet,

**RVC: Recipient Verify Check**

Der RVC-Filter prüft bereits während der E-Mail-Annahme (SMTP-Server-Dialog), ob die Empfängeradresse auf dem Zielsystem überhaupt bekannt ist. Falls nicht, wird der Empfang bereits während des Zustellversuches abgelehnt. Dadurch werden Spam-Attacken auf nicht

existierende Postfächer abgefedert, ohne die Leistung Ihrer E-Mail-Server zu beeinträchtigen. Die Quittierung erfolgt dabei mit: 550 Recipient not accepted (Unknown recipient: <xxxx@domain.tld>).

### 4.4.2.5 CISS

**Die Innovation des REDDOXX Spamfinders heißt CISS**

CISS (Confirmation Interactive Site Server) ist ein einmaliger, mehrstufiger Kontrollvorgang, der den dauerhaften Austausch von erwünschten E-Mails zwischen Sender und Empfänger sicherstellt.
**Stufe 1:** E-Mail-Empfang, Prüfung auf Viren und Spam durch Anti-Spam-Filter und Ablage in temporären Speicher. Versand einer Antwort-E-Mail an den Absender mit der Bitte um einmalige Autorisierung unter dem angegebenen Link.
**Stufe 2:** Aufforderung auf der Internetseite eine bestimmte Aktion auszuführen, die nur von einem Menschen, nicht aber von Spam-Robots ausgeführt werden kann.
**Stufe 3:** Rückmeldung vom Portal an den REDDOXX Spamfinder über die erfolgreiche Autorisierung und automatische Weiterleitung der E-Mail an den Empfänger.

**Wie funktioniert der CISS Vorgang?**

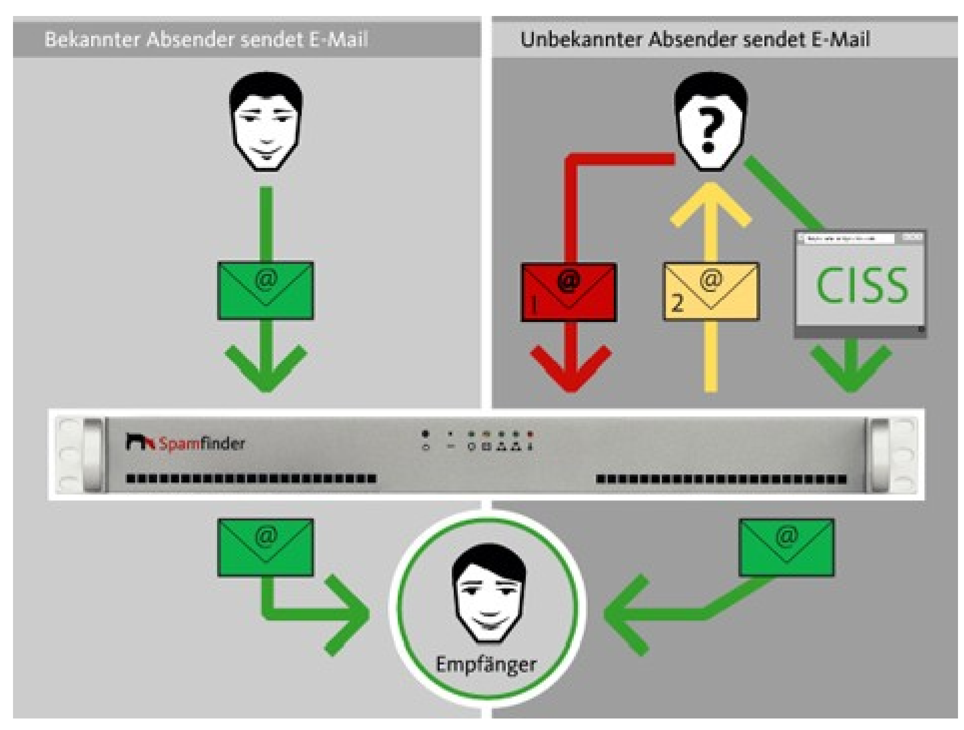



Abbildung: CISS Schema

**Bekannter Absender sendet E-Mail:**

1. Ein Kunde oder Geschäftspartner schreibt Ihnen eine E-Mail.
2. Die REDDOXX Appliance prüft diese E-Mail im Hinblick auf Viren, Würmer, Trojaner und natürlich auch ob es sich um Spam handelt.
3. Nach dieser Prüfung wird die E-Mail umgehend an Sie weitergeleitet.

**Unbekannter Absender sendet E-Mail:**

4. Eine unbekannte Person schreibt Ihnen eine E-Mail.
5. Die REDDOXX Appliance prüft diese E-Mail im Hinblick auf Viren, Würmer, Trojaner und natürlich ob es sich um Spam handelt. Da der Absender unbekannt ist, wird die E-Mail temporär gespeichert. Der Spamfinder generiert eine E-Mail an den Absender mit der Bitte um eine einmalige Autorisierung unter einem dort angegebenen Link.
6. Auf dieser Internetseite wird der Absender gebeten, eine bestimmte Aktion auszuführen, wie zum Beispiel auf einen bestimmten Bereich eines Bildes zu klicken.
7. Aktionen dieser Art können nur von Menschen, nicht aber automatisiert ausgeführt werden.
8. Diese Aktion generiert eine Rückmeldung an die REDDOXX Appliance über die erfolgreiche Autorisierung des Absenders.
9. Die gespeicherte E-Mail wird direkt an Sie weitergeleitet und einem neuen Auftrag steht nichts mehr im Weg!

### 4.4.2.6 Filtereinstellungen

Über die Filterkonfiguration können Sie die einzelnen Filter konfigurieren.

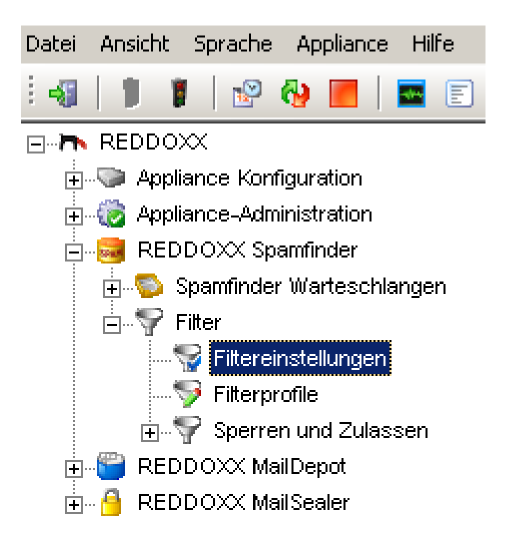



Abbildung: Navigationsbaum: Filtereinstellungen

**Allgemeine Filterkonfiguration**

Klicken Sie in der Baumansicht auf ***Filter - Filtereinstellungen*** doppelt. Es öffnet sich ein Fenster mit dem Reiter *Allgemein*.

Folgende Felder werden im Bereich Konfiguration angezeigt:

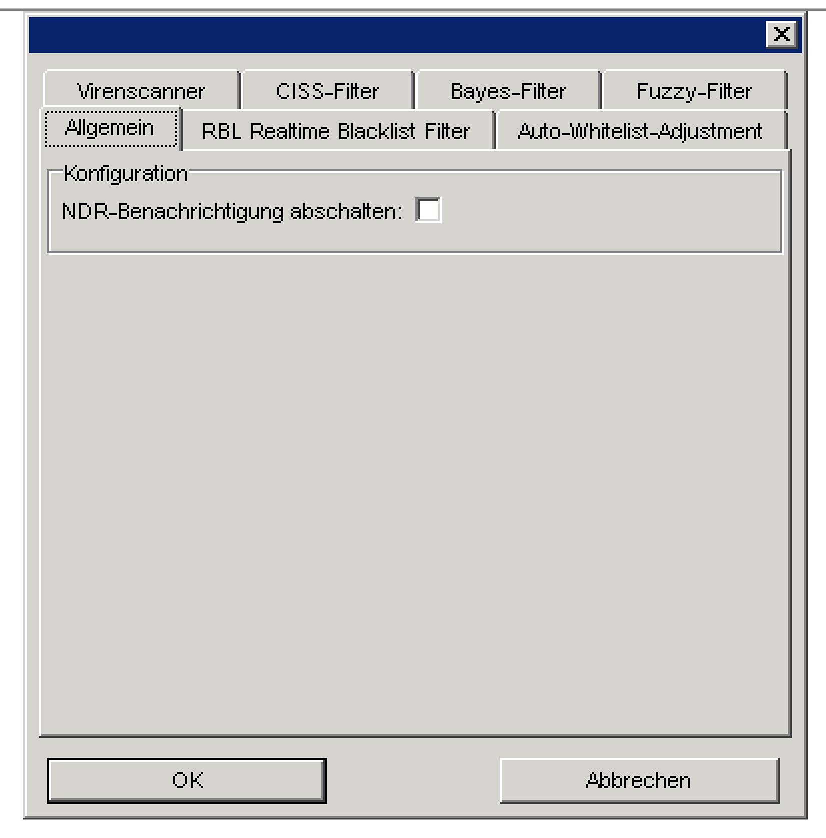



Abbildung: Filterkonfiguration – Allgemein

1. NDR-Benachrichtigung abschalten:
Schalten Sie die NDR-Benachrichtung ab, wenn Sie Nachrichten, die von Ihrem Mailserver oder von Ihrer Appliance abgelehnt werden und üblicherweise als NDR-Nachricht zurückgesendet werden, verwerfen wollen. Die ausgehende NDR-Nachricht wird gelöscht und nicht versendet. Dies verhindert, dass ausgehende NDR-Nachrichten, die selbst nicht zustellbar sind, unnötigerweise die Ausgangswarteschlange der Appliance blockieren und unübersichtlich werden lassen.

**Realtime Blacklist Filter**

Beim Realtime Blacklist Filter handelt es sich um einen DNS Blacklist Filter. Beim Advanced Realtime Blacklist Filter handelt es sich um einen Extended DNS Blacklist Filter. Den Advanced Realtime Blacklist Filter können Sie folgendermaßen konfigurieren.

1. Klicken Sie in der Baumansicht auf ***Filter - Filtereinstellungen*** doppelt.
   Folgende Felder werden angezeigt:

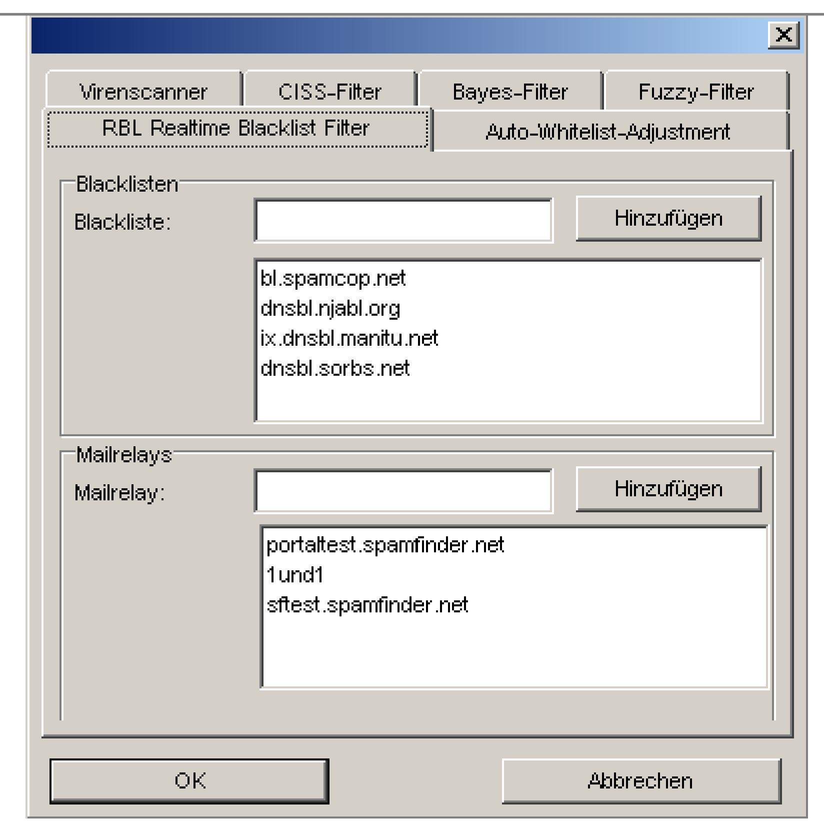



Abbildung: Filterkonfiguration - Realtime Blacklist Filter

2. Geben Sie eine Blacklist an, welche der entsprechende Filter abfragen soll.
3. Fügen Sie mit der Schaltfläche HINZUFÜGEN die Blacklist zu der Liste hinzu.
4. Fügen Sie mit der Schaltfläche HINZUFÜGEN die Relays der Liste hinzu, denen Sie innerhalb ihres Mailflow vertrauen. Den Namen eines Relays erhalten Sie z.B. aus dem Header einer E-Mail (z.B. mail.company.net).




Abbildung: Header einer E-Mail

5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Auto Whitelist Adjustment konfigurieren**

Dieser Filter fügt den Empfänger der ausgehenden E-Mails der Sender Adressen Whitelist hinzu.

1. Wählen Sie den Reiter **– *Auto-Whitelist-Adjustment*** aus.
   Folgende Felder werden angezeigt:

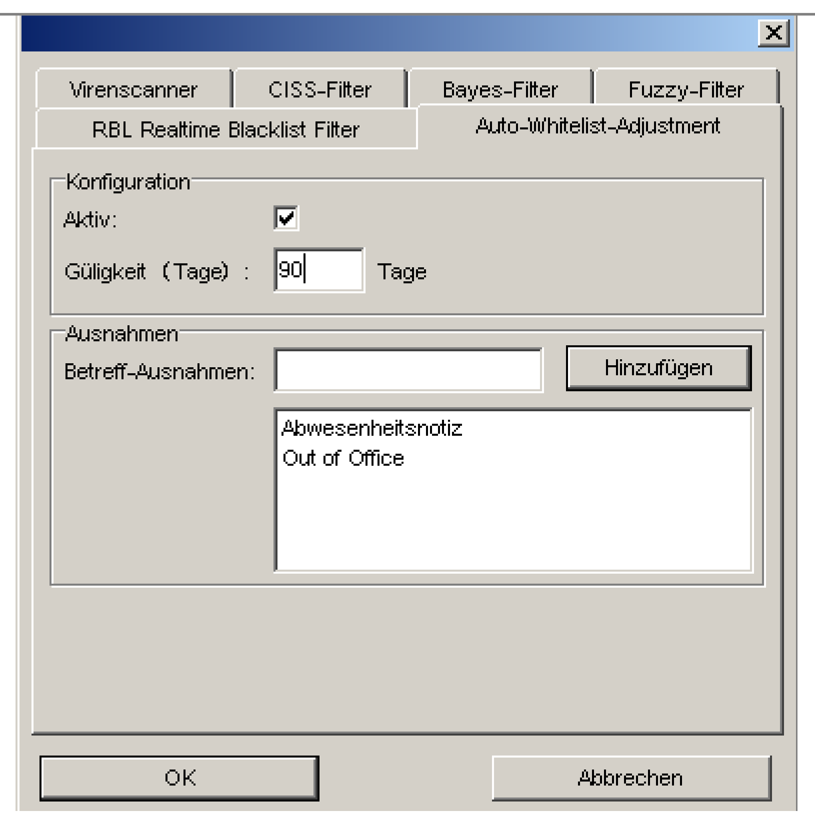



Abbildung: Filterkonfiguration – Auto-Whitelist-Adjustment

2. Aktivieren Sie bei Bedarf den Filter.
3. Geben Sie die gewünschte Gültigkeit in Tagen an.

**HINWEIS**

Whitelists sollten eine Gültigkeit von mindestens 90 Tagen besitzen.

4. Um zu verhindern, dass die Absenderadresse eines Spam-Versenders wegen einer automatischen Antwort Ihres Postfachs in die White List eingetragen wird, können Sie das Whitelisten für beliebige Betreffangaben, wie z.B. Urlaub, Abwesenheitsnotiz, (Out of Office), etc. unterbinden. Tragen Sie dazu einen Teil oder den gesamten Betreff in das Betreff-Ausnahmefeld ein. Diese Einstellung gilt global für alle Benutzer.

**HINWEIS**

Der Empfänger der ausgehenden E-Mails kann allerdings nicht für AutoResponder konfiguriert werden, benutzen Sie dazu die Ausnahmefunktion.

5. Fügen Sie mit der Schaltfläche HINZUFÜGEN die Ausnahme der Liste hinzu.
   Mit der ENTF-Taste kann eine beliebige schon eingetragene Ausnahme wieder gelöscht werden.
6. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Virenscanner konfigurieren**

Bei der Konfiguration des Virenscanners können Sie einstellen, an wen Benachrichtigungen gesendet werden. Hier können Sie auch Dateiendungen für Anhänge angeben, die nicht durchgelassen werden sollen.

**Einschränkung:** Nur der Virenscanner kann auf folgende Weise konfiguriert werden.

2. Wählen den Reiter ***Virenscanner*** aus.
 Folgende Felder werden angezeigt:

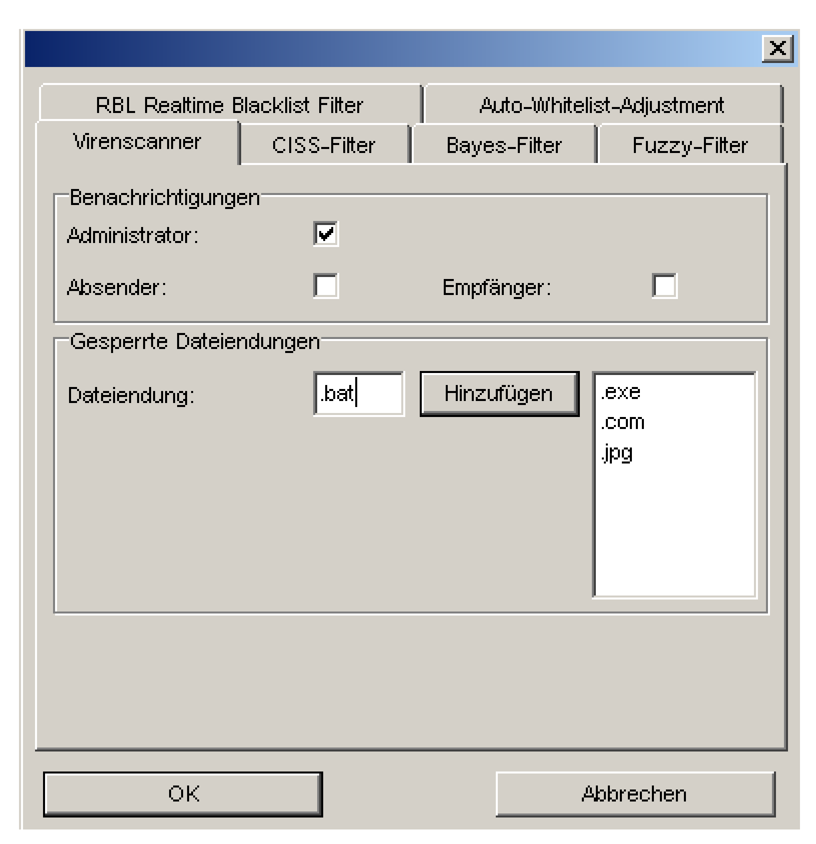



Abbildung: Filterkonfiguration - Virenscanner

3. Aktivieren Sie die Zielperson(en), die eine Benachrichtigung erhalten soll(en).
4. Geben Sie die zu sperrenden Dateiendungen mit einem führenden Punkt ein (z.B. „.exe“) und klicken Sie auf *Hinzufügen.*
5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
 ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

| HINWEIS |
| --- |
| Achten Sie bitte darauf, dass der Eintrag bei Dateiendung mit einem Punkt (.) beginnt. |

### CISS Filter konfigurieren

Bei der Konfiguration des CISS Filters können Sie die Whitelist-Gültigkeit in Tagen festlegen und die maximalen Challenges pro Absender. Mit Challenges beschreibt man die Versuche eines Absenders eine E-Mail zum xten Mal (hier 3-mal) an denselben Empfänger zu senden, ohne dass der Empfänger darauf antwortet.

**Einschränkung:** Nur der CISS Filter kann auf folgende Weise konfiguriert werden.

1. Wählen Sie den Reiter ***CISS Filter*** aus.
 Folgende Felder werden angezeigt:

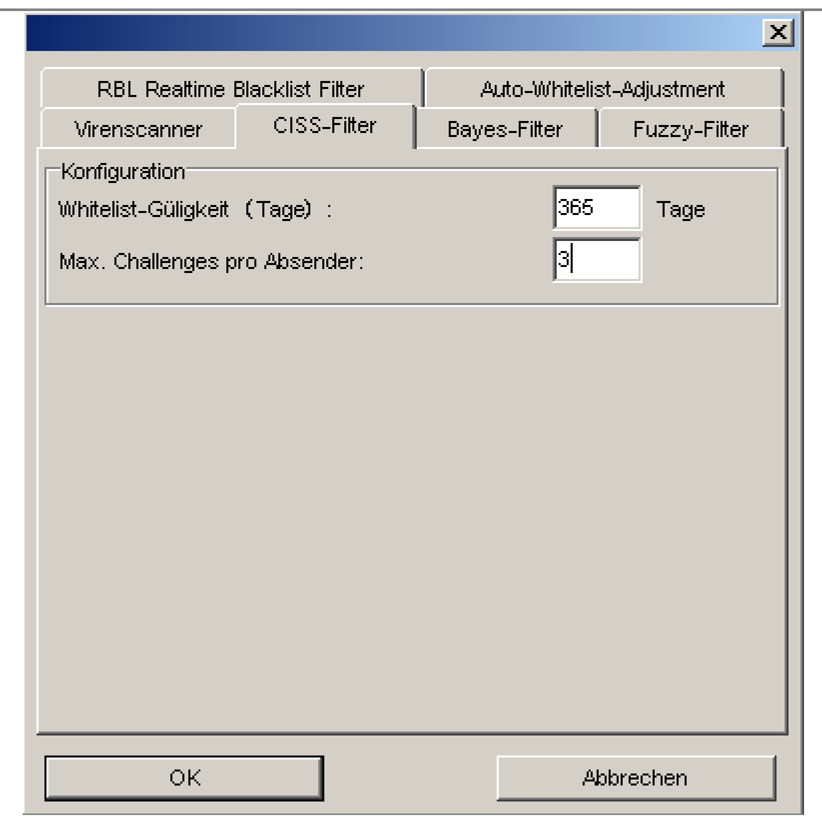



Abbildung: Filterkonfiguration - CISS Filter

3. Geben Sie die gewünschte Whitelist-Gültigkeit für den CISS Filter in Tagen an. Der Standard ist 365 Tage.
4. Geben Sie die maximalen Challenges pro Absender an. Der Standard ist 3.
5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Bayes-Filter**

Bei der Konfiguration des Bayes Filters können Sie die Bayes-Datenbank löschen und das automatische Training des Filter aktivieren oder deaktivieren

1. Wählen Sie den Reiter ***Bayes Filter*** aus.
   Folgende Felder werden angezeigt:

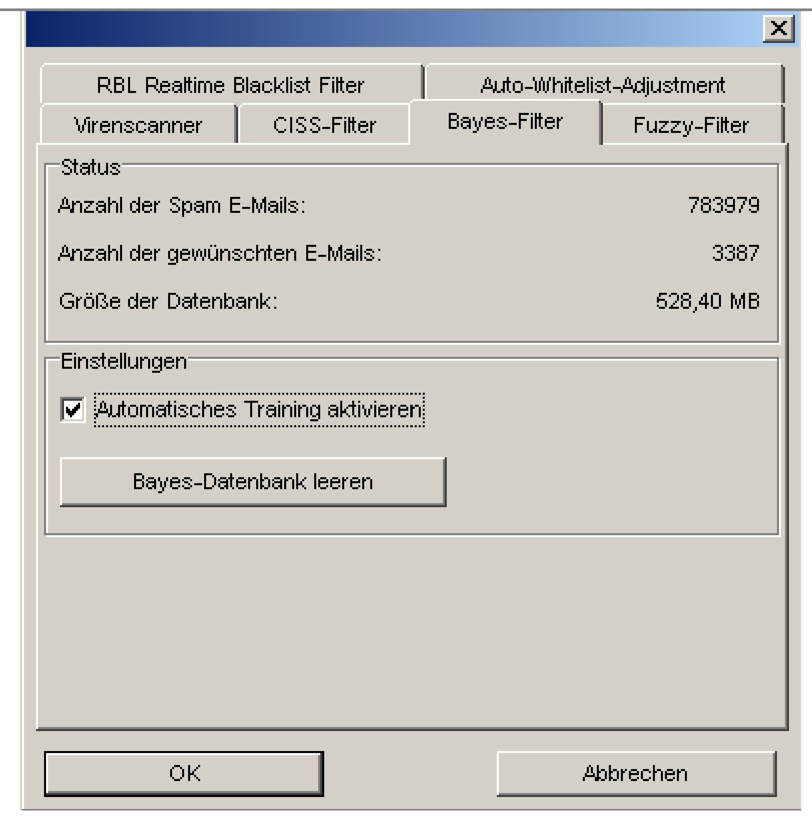



Abbildung: Filterkonfiguration - Bayes Filter

2. Im Status ist die Anzahl der Mails hinterlegt, welche dem Bayesfilter als Basis dienen. Dabei wird zwischen Spam und erwünschten E-Mails unterschieden. Zusätzlich wird die physikalische Größe dieser Mails in der Datenbank angezeigt.
3. Automatisches Training aktivieren:
   Bevor Sie den Bayes-Filter einsetzen, sollte dieser zuerst für ca. 1 Woche trainiert werden. Dabei lernt der Filter anhand von Black- und Whitelisten, welche E-Mails erwünscht bzw. unerwünscht sind und baut anhand der Inhalte die Filter-Datenbank auf.

   Details zur Funktionsweise des Bayes-Filters finden Sie unter dem Kapitel Filtereinstellungen.

4. Bayes-Datenbank leeren:
   Durch anfängliche Konfigurationsfehler der REDDOXX oder falscher Einträge in den Black- und Whitelisten kann es vorkommen, dass der Bayes-Filter Inhalte als SPAM klassifiziert und in seine Datenbank übernommen hat und somit gewünschte E-Mails als SPAM meldet, oder unerwünschte E-Mails nicht erkennt. In diesem Fall sollten Sie die Konfiguration der REDDOXX und die Black- und Whitelisten überprüfen. Danach können Sie die Datenbank leeren und neu aufbauen (=trainieren) lassen.

**HINWEIS**

Nach einer Woche Training für den Bayes-Filter sollten die beiden Werte für Spam-E-Mails bzw. Anzahl gewünschter E-Mails positive Zahlen anzeigen. Je größer die beiden Werte, umso genauer wird der Filter arbeiten. Sollte die Datenbank einmal zu groß werden (Abhängig von der Hardwareausstattung Ihrer REDDOXX Appliance), kann dies die Verarbeitungsgeschwindigkeit beinträchtigen. In solch einem Fall können Sie die Datenbank leeren und erneut trainieren lassen. Sie sollten den Bayes-Filter zuerst trainieren, bevor Sie in als aktiven Filter einsetzen.

**Fuzzy-Filter**

Der Fuzzy Filter arbeitet überwiegend vollautomatisch. Lediglich beim Versand von Massen-E-Mails kann es zu sogenannten *„False Positives“* kommen.

1. Wählen Sie den Reiter ***Fuzzy Filter*** aus.
   Folgende Felder werden angezeigt:

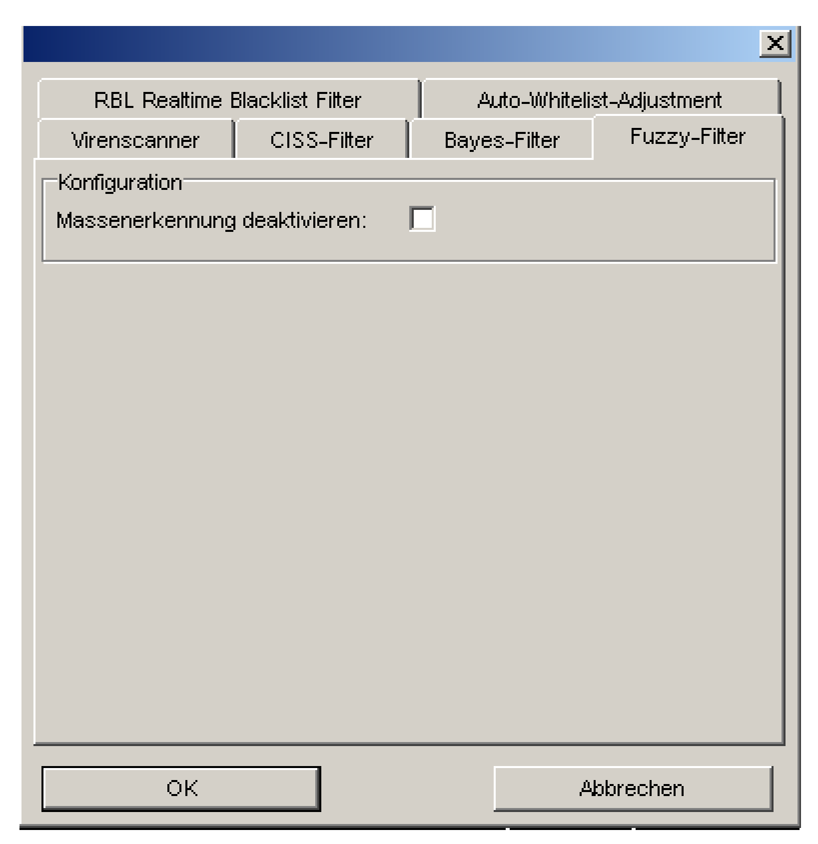



Abbildung: Filterkonfiguration - Fuzzy Filter

2. Massenerkennung deaktivieren:
   Deaktivieren Sie diese Funktion, wenn fälschlicherweise Massen-E-Mail (z.B. Newsletter) als Spam erkannt werden.

### 4.4.2.7 Filterprofile

Das Herzstück des Spamfinders liegt in seinen Filterprofilen. Hier können Sie die Filterregeln gemäß Ihrem Spam-Aufkommen einstellen.
Sie können neue Profile erstellen, vorhandene Profile ändern, kopieren oder auch löschen. Sie bestimmen hier, welche Filter einem Profil zugeordnet werden und welche Profile dem Benutzer zur Auswahl stehen sollen. Sowohl der Administrator als auch der Benutzer (sofern freigegeben), kann Filterprofile zu E-Mail-Aliase zuordnen.

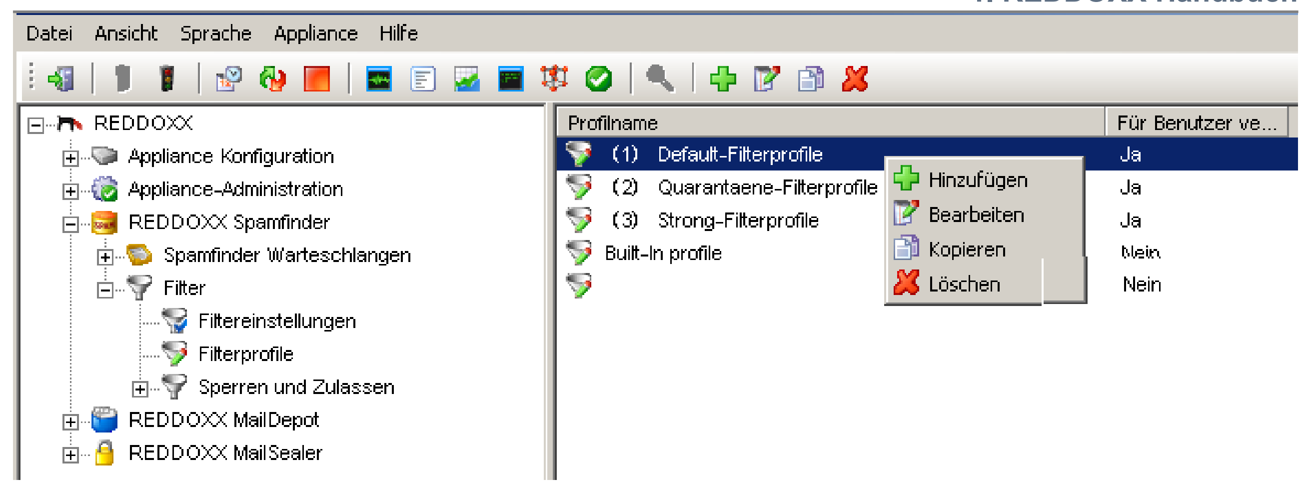



Abbildung: Filterprofile

**vordefinierte Filterprofile**

Die REDDOXX verfügt über 4 vordefinierte Filterprofile. Sie beinhalten in der Grundkonfiguration immer die Positivfilter DWL, AWL und SWL.

**Default Filterprofil**

Das Default-Profil beinhaltet zu Beginn die Filter FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC. Bei der automatischen Benutzer- und E-Mail-Alias-Erstellung wird zuerst immer das Default-Filterprofil zugeordnet. Stellen Sie dieses Profil so ein, dass es den Anforderungen der meisten Benutzer in Ihrem Unternehmen entspricht. Durch die automatische E-Mail-Alias-Erstellung mit automatischer Zuordnung zum Default-Filterprofil wird der Administrationsaufwand deutlich reduziert.

**Quarantäne-Filterprofil**

Das Quarantäne-Profil beinhaltet zunächst die Filter FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC und BAYES. Sie können dieses Profil so anpassen, dass es den vom Default-Profil abweichenden Anforderungen entspricht.
Die Aktionen der meisten dieser Filter stehen auf Quarantäne. Bayes und SRC stehen auf Markieren.

**Strong-Filterprofil**

Das Strong-Filterprofil beinhaltet die Filter FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC und CISS. Dieses Profil ist für Benutzer vorgesehen, die sofort einen zuverlässigen Spamschutz haben möchten. Dies wird durch den CISS-Filter gewährleistet.

**Built-In Profil**

Das *Built-In Profil* wird benutzt, wenn dem E-Mail-Alias noch kein Filterprofil zugeordnet ist. Voraussetzung dafür ist die generelle Aktivierung des Profils (siehe Kapitel 4.2.3.6). Es kann nicht verändert werden. Es signalisiert dem Administrator, dass die REDDOXX zwar im Einsatz ist, aber nicht ausreichend konfiguriert ist, oder dass, generell – oder für diesen Benutzer - keine Lizenzen vorhanden sind. Das Built-In Profil beinhaltet nur die Filter RBL, ARBL und FUZZY. Erkannte Spam-E-Mails werden mit dem TAG [REDDOXX Spamfinder] markiert, ein abweichender TAG ist nicht möglich.

### Neues Filterprofil anlegen

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht ***Filterprofile*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Hinzufügen**.
   Folgende Felder werden angezeigt:

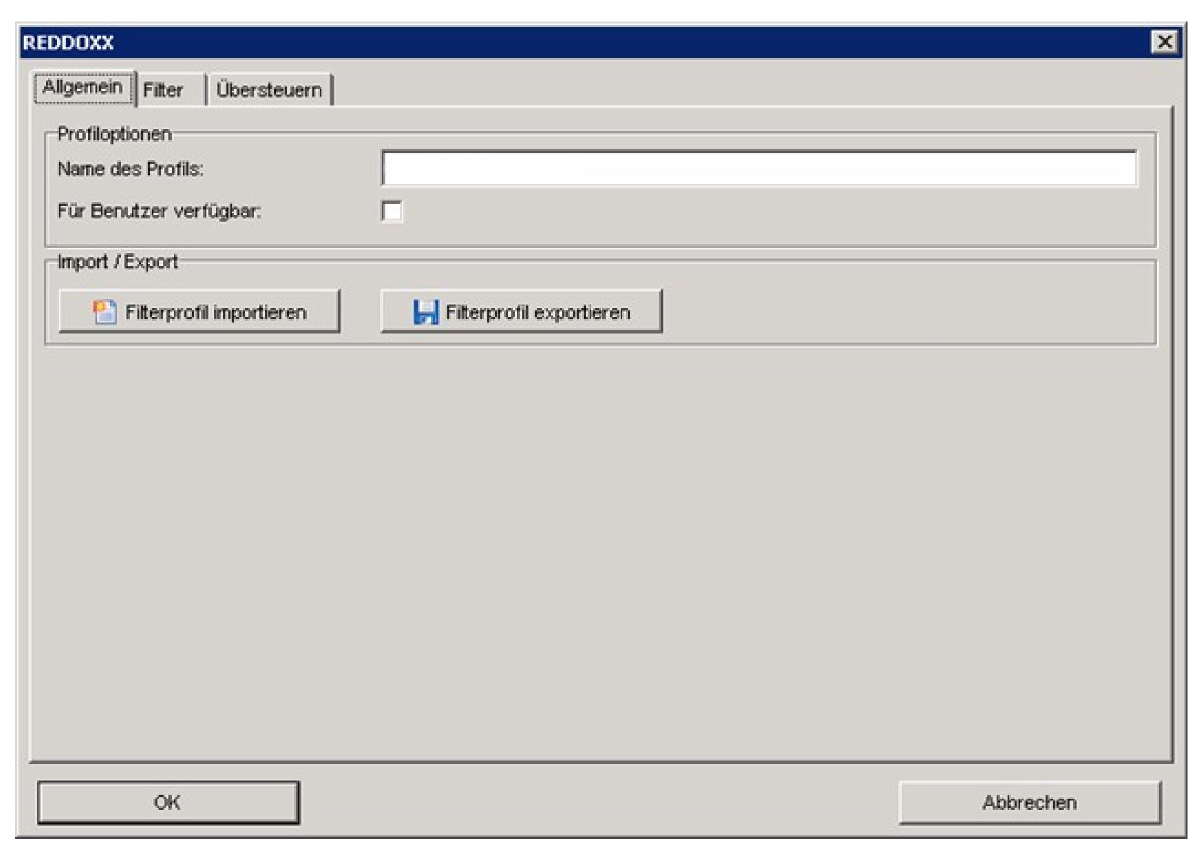



Abbildung: Filterprofile - Reiter "Allgemein"

**HINWEIS**

Der Profilname wird in der Listenansicht alphabetisch angezeigt. Sie können durch gezieltes Voranstellen von Nummern oder Gruppenkennzeichen Ihre eigene Sortierreihenfolge bestimmen.

4. Geben Sie bei den Profiloptionen *Name des Profils* ein.
5. Aktivieren Sie die Option *Für Benutzer verfügbar*, wenn Sie das Filterprofil für die Benutzer ebenfalls verfügbar machen möchten. Der Benutzer kann dann dieses Filterprofil für seine E-Mail-Adressen in der User-Konsole auswählen.
6. Importieren oder exportieren Sie gegebenenfalls Filterprofile.
   Exportieren Sie Ihre gewünschten Filterprofile, um sie auf einer anderen REDDOXX Appliance (z.B. Tochterunternehmen) importieren zu können.

### Filter

Verschiedene Filter können ausgewählt und nach Priorität zusammengestellt werden.

**Voraussetzung:** Keine.

1. Klicken Sie auf den Reiter "Filter".
   Folgende Felder werden angezeigt:

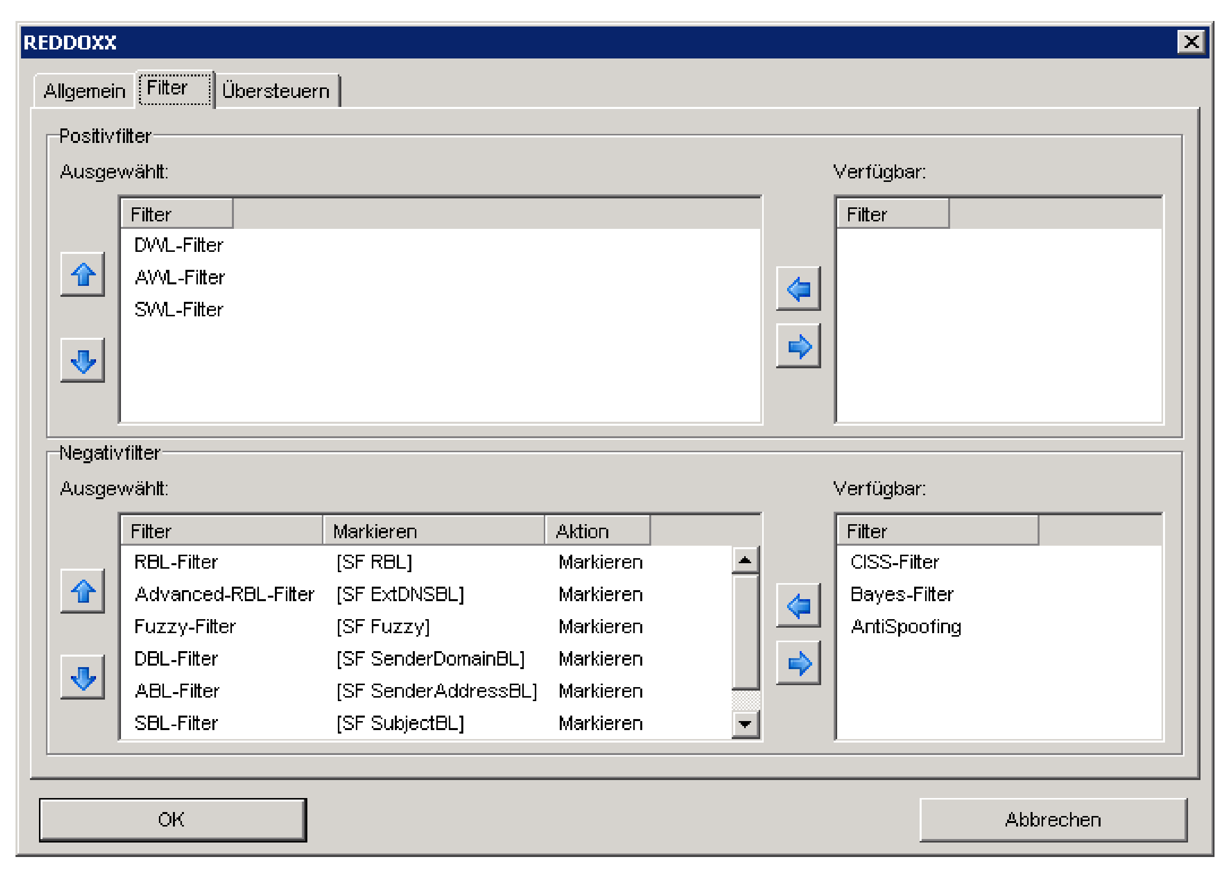



Abbildung: Filterprofile - Reiter "Filter"

2. *Positivfilter - Ausgewählt:*
   Im Feld *Ausgewählt* sind alle aktiven Positivfilter gelistet. Über die vertikalen Pfeile können Sie die Reihenfolge der Filter ändern. Markieren Sie dazu den gewünschten Filter und klicken auf die entsprechende Schaltfläche. Über die vertikalen Pfeile können Sie die Reihenfolge der Filter ändern.
   Reihenfolge: von oben nach unten, oben zuerst.
3. *Positivfilter - Verfügbar:*
   Im Feld *Verfügbar* sind alle verfügbaren Positivfilter gelistet. Über die horizontalen Pfeile können Sie die verfügbaren Filter zu der Liste der ausgewählten Filter hinzufügen und umgekehrt. Markieren Sie dazu den gewünschten Filter und klicken auf die entsprechende Schaltfläche. Über die vertikalen Pfeile können Sie die Reihenfolge der Filter ändern.
   Reihenfolge: von oben nach unten, oben zuerst.
4. *Negativfilter:*
   Für die Felder "Ausgewählt und "Verfügbar" gilt gleiches wie bei Positivfilter (Punkt 2-3). Zudem können Sie den einzelnen Negativfiltern 3 verschiedene Aktionen zuweisen. Um eine Aktion zuzuweisen oder zu verändern klicken Sie bitte doppelt auf einen Filter.
   Folgendes Fenster wird angezeigt:




Abbildung: Filterprofile - Reiter "Filter" – Aktion

5. *Tag:* Tag (engl. Markierung) ist ein Text, welcher einer E-Mail im Betreff-Feld vorangestellt wird, sollte die gewünschte Aktion auf MARKIEREN ausgewählt sein. Andere Aktionen verändern den Betreff nicht.
6. *Aktion:* In dieser Auswahlliste können Sie zwischen 3 Aktionen wählen:
   1. Markieren: Markiert die E-Mail im Betreff-Feld mit dem eingetragenen Tag. Der Tag wird dabei dem Betreff vorangestellt und die E-Mail wird zugestellt.
   2. Quarantäne: Die E-Mail wird in das geschützte Quarantäne-Verzeichnis verschoben und dem Empfänger nicht zugestellt. Alle E-Mails in Quarantäne können in den *Spamfinder-Warteschlangen* gefunden werden.
   3. Ablehnen: Die E-Mail wird abgelehnt und somit nicht dem Empfänger zugestellt. Der Absender erhält eine Bounce-E-Mail.

**HINWEIS**

Greifen mehrere Negativfilter, so wird jene Aktion ausgelöst, welche am stärksten gewichtet ist.

Reihenfolge der Gewichtung: MARKIEREN (leicht) - QUARANTÄNE (mittel) - ABLEHNEN (schwer).

Beachten Sie beim Antispoofing-Filter, dass die Markierung nicht auf ABLEHNEN steht, da sonst eine Bounce-E-Mail erzeugt wird, die möglicherweise an Sie selbst versendet wird, weil als Absender Ihre Adresse angegeben wurde.

### Reihenfolge der Filter

Die Filterreihenfolge wird durch die Performance-Relevanz und False-Positive-Rate des Filters bestimmt.
Die ausgewählten Negativfilter werden von oben nach unten durchlaufen. Greift bei einem Filter die Aktion ABLEHNEN, so werden keine weiteren Filter mehr durchlaufen:

| FILTER | AKTION |
|---|---|
| Anti-Spoofing | Quarantäne |
| Fuzzy | Quarantäne |
| RBL | Quarantäne |
| Advanced RBL | Quarantäne |
| SBL | Markieren |
| ABL | Markieren |
| DBL | Markieren |
| SRC | Markieren |
| Bayes | Quarantäne |
| CISS | Quarantäne |

Abbildung: Empfohlene Filterreihenfolge

### Filter übersteuern

Sollen ausdrücklich erwünschte E-Mails (White-Listeintrag) ohne weitere Prüfung auf SPAM-Relevanz zugestellt werden, so müssen die Negativfilter durch die jeweiligen Postivfilter (DWL, AWL, SWL) übersteuert werden. Als Ausnahme gilt dabei der Antispoofing-Filter.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht ***Filterprofile*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste auf ein Profil.
3. Klicken Sie auf den Reiter "Übersteuern".
   Folgende Felder werden angezeigt:

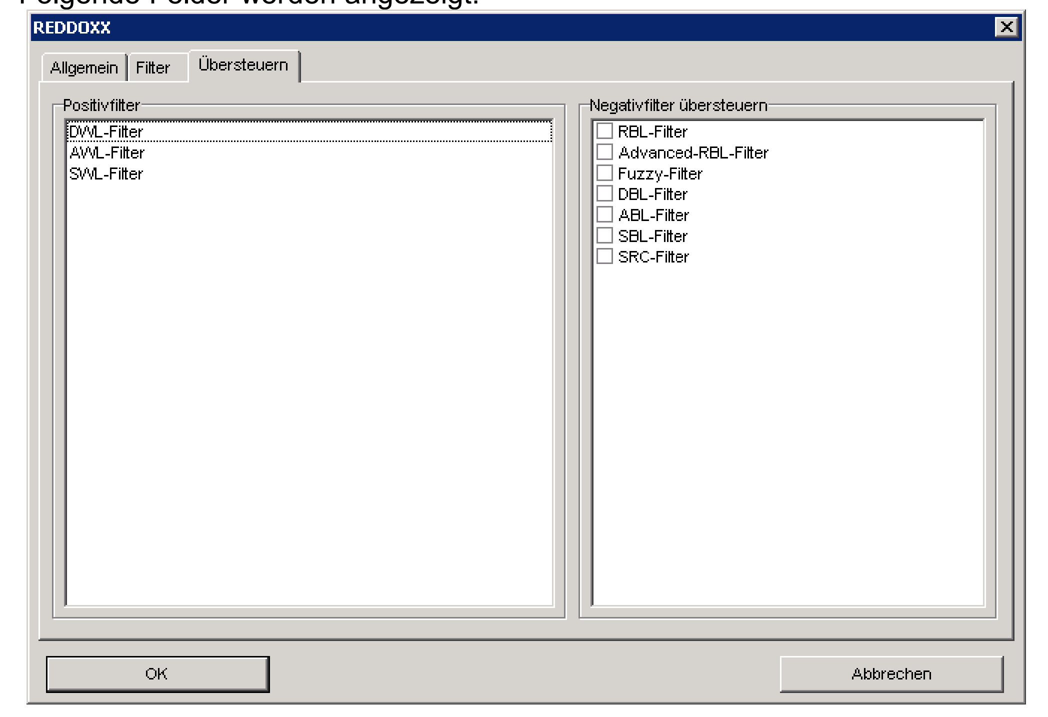



Abbildung: Filterprofile - Reiter "Übersteuern"

4. Wählen Sie aus, welche Positivfilter die Negativfilter übersteuern. Wird ein Negativfilter von einem
   Positivfilter übersteuert, so hat der Negativfilter keine Relevanz mehr.

**HINWEIS**

Insbesondere beim CISS-Filter MUSS der AWL-Filter den Negativfilter CISS übersteuern, da sonst immer wieder die CISS-Challenge erzeugt wird.

5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### Filterprofil bearbeiten

Hier können Sie schon angelegt Filterprofile bearbeiten.

**Voraussetzung:** Angelegtes Filterprofil vorhanden.

1. Wählen Sie in der Baumansicht ***Filterprofile*** aus.
2. Klicken Sie die zu bearbeitende E-Mail mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Bearbeiten**.
4. Nehmen Sie die gewünschten Änderungen vor.

5. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Filterprofil kopieren**

Hier können Sie schon angelegt Filterprofile kopieren.
**Voraussetzung:** Angelegtes Filterprofil vorhanden.

1. Wählen Sie in der Baumansicht ***Filterprofile*** aus.
2. Klicken Sie die zu kopierende E-Mail mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Kopieren**.
4. Klicken Sie doppelt auf das Filterprofil mit dem Zusatz (copy).
5. Geben Sie bei den Profiloptionen den Namen des neuen Filterprofils ein.
6. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

**Filterprofil löschen**

Hier können Sie schon angelegt Filterprofile löschen.
**Voraussetzung:** Angelegtes Filterprofil vorhanden.

1. Wählen Sie in der Baumansicht ***Filterprofile*** aus.
2. Klicken Sie die zu bearbeitende E-Mail mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit JA, um die E-Mail zu löschen.
   NEIN: E-Mail wird nicht gelöscht.

### 4.4.2.8 Sperren und Zulassen

**Sperren und Zulassen (Black- und White-Listen)**

Folgende Punkte gelten für alle nachfolgend beschriebenen Listen:

**Global oder Userbezogen**
Die Einstellungen für die Black- und Whitelisten in der Administrator-Konsole gelten global, d.h. für alle Benutzer. Gibt es zutreffende Black/White-Listeinträge auch beim User, so haben diese Vorrang vor den globalen Einstellungen. So kann es sein, dass eine globale Sperre auf ABLEHNEN steht, der User aber die Sperre auf MARKIEREN eingestellt hat. Es gilt die Regel: Der User gewinnt immer!
Für alle Blacklisten gilt: Die bei einer Sperre ausgewählte Aktion gilt. Die Einstellung beim Filterprofil selbst hat keine Relevanz.

**Gültigkeits-Datum**
Achten Sie darauf ein gültiges Datum in der Zukunft zu wählen, da sonst der Eintrag nicht greift. Derzeit gibt es noch keine Ablauf-Benachrichtigungen. Das Vorgabedatum ist HEUTE + 365 Tage.

**Groß/Kleinschreibung**
Die Groß/Kleinschreibung bei E-Mail-Adressen, Domänen-Namen und Betreffzeilen (Subjects) wird nicht beachtet.

**Umlaute**
Umlaute bei den Betreffzeilen werden seit Version 1022 unterstützt.

**HINWEIS**

IP-basierte Blacklists finden Sie unter SMTP-Einstellungen - Gesperrte IP-Adressen. Diese gelten systemweit und sind profilneutral.

### DWL Domänen Whitelist neu anlegen

Über die Filterlisten können Sie neue Domänen Whitelists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - DWL Domain Whitelist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

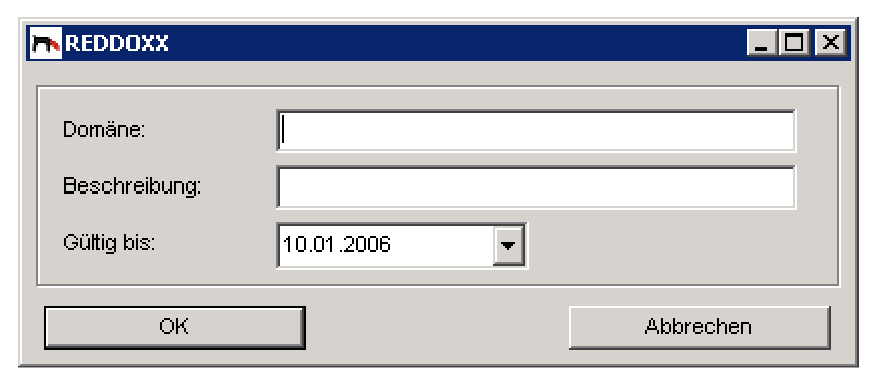



Abbildung: Sperren und Zulassen - DWL Domain Whitelist

4. Geben Sie eine *Domäne* an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Klicken Sie auf das Kalenderblatt, wenn Sie einen Kalender zur Auswahl des Datums benötigen.
6. Kommentieren Sie den Filter bei Bedarf.
7. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### DBL Domain Blacklist neu anlegen

Über die Filterlisten können Sie neue Domänen Blacklists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - DBL Domain Blacklist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.

3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

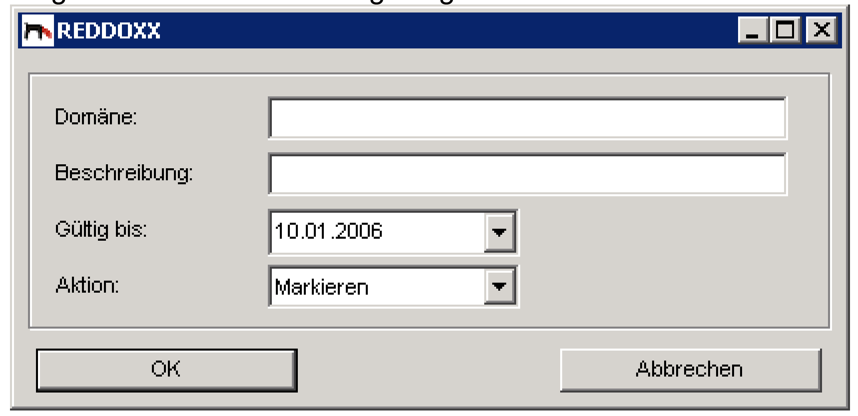



Abbildung: Sperren und Zulassen - DBL Domain Blacklist

4. Geben Sie eine *Domäne* an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Klicken Sie auf das Kalenderblatt, wenn Sie einen Kalender zur Auswahl des Datums benötigen.
6. Wählen Sie über die Auswahlliste die *Aktion* für den Filter aus.
   Die Einstellungen Markieren, Quarantäne und Ablehnen sind möglich.
7. Kommentieren Sie den Filter bei Bedarf.
8. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### AWL Address Whitelist neu anlegen

Über die Filterlisten können Sie neue Adressen Whitelists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - AWL Address Whitelist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

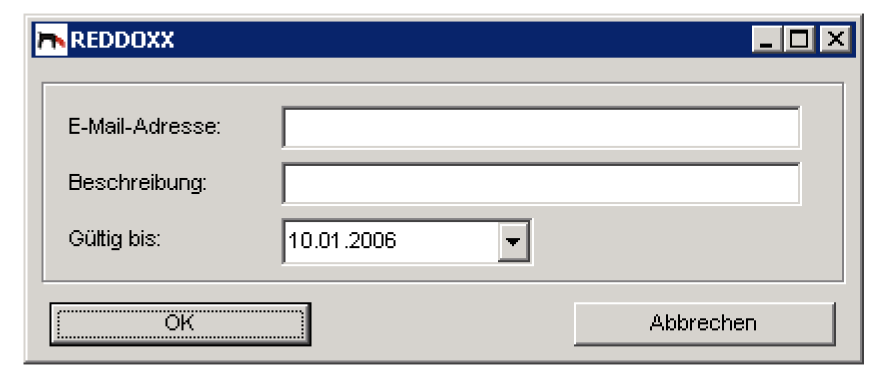



Abbildung: Sperren und Zulassen - AWL Address Whitelist

4. Geben Sie die gewünschte *E-Mail-Adresse* an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Klicken Sie auf das Kalenderblatt, wenn Sie einen Kalender zur Auswahl des Datums benötigen.
6. Kommentieren Sie den Filter bei Bedarf.

7. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### AWL Address Whitelist importieren

Hiermit können Sie E-Mail-Adressen in die Address-Whitelist importieren.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - AWL Address Whitelist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Adressen importieren**.
   Folgende Felder werden angezeigt:

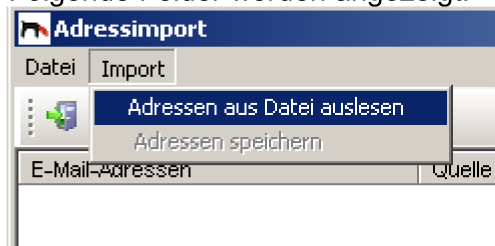



Abbildung: Sperren und Zulassen - AWL Adressimport

4. Wählen Sie „Adressen aus Datei lesen“ aus.
5. Im Dialogfeld - Dateiauswahl - wählen Sie die zu importierende Datei aus.
   Format: Pro Zeile – eine E-Mailadresse. Die Adresse muss gültig (@-Zeichen) sein. Die Zeile muss mit einem CR – Line Feed – abgeschlossen sein, auch die letzte Zeile. Ungültige Adressen, wie zum Beispiel Kommentare, werden übersprungen.
   Folgende Liste wird angezeigt: (Beispiel)

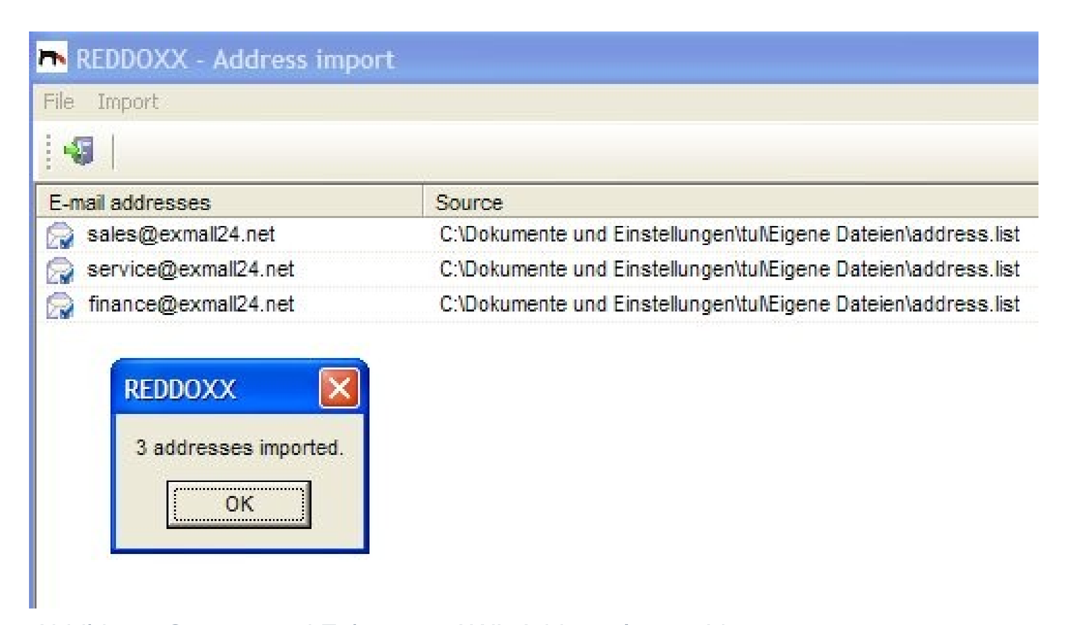



Abbildung: Sperren und Zulassen - AWL Address Import Liste

6. Wählen Sie im Menü: Import – Adressen speichern – aus. Die Adressen werden nun in die Whitelist importiert. Sie erhalten eine Kontroll-Meldung, wie viele Adressen importiert wurden.

### ABL Address Blacklist neu anlegen

Über die Filterlisten können Sie neue Address-Blacklists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht ***Sperren und Zulassen - ABL Address Blacklist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

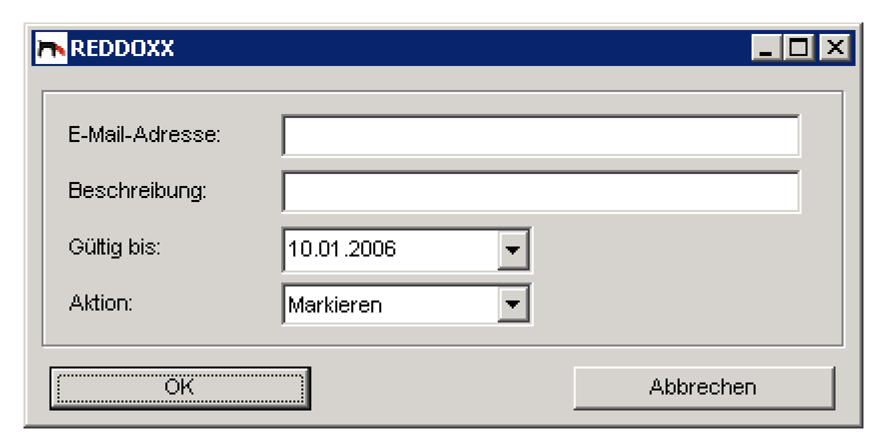



Abbildung: Sperren und Zulassen - ABL Address Blacklist

4. Geben Sie die gewünschte *E-Mail-Adresse* an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Klicken Sie auf das Kalenderblatt, wenn Sie einen Kalender zur Auswahl des Datums benötigen.
6. Wählen Sie über die Auswahlliste die *Aktion* für den Filter aus.
   Die Einstellungen Markieren, Quarantäne und Ablehnen sind möglich.
7. Kommentieren Sie den Filter bei Bedarf.
8. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### SWL Betreff Whitelist neu anlegen

Über die Filterlisten können Sie neue Betreff- Whitelists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - SWL Betreff Whitelist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

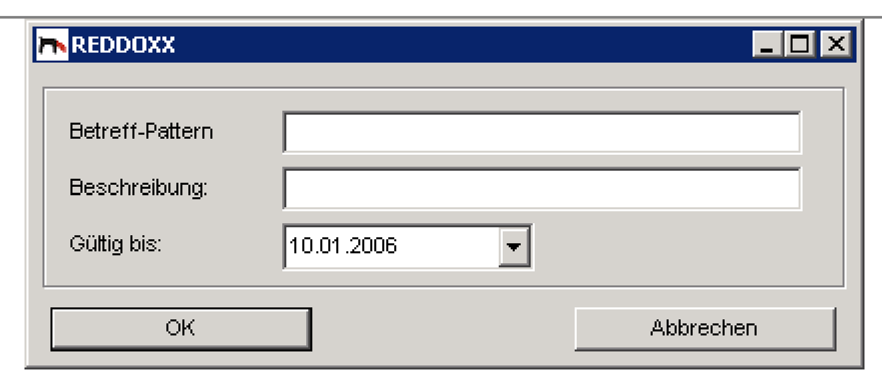



Abbildung: Sperren und Zulassen - SWL Betreff Whitelist

4. Geben Sie eine Zeichenfolge an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Die Vorbelegung lautet: Heute + 365 Tage
   Klicken Sie auf die Auswahlliste *Gültig bis,* wenn Sie einen Kalender zur Auswahl des Datums benötigen.
6. Kommentieren Sie den Filter bei Bedarf.
7. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

### SBL Betreff Blacklist neu anlegen

Über die Filterlisten können Sie neue Betreff- Blacklists anlegen.

**Voraussetzung:** Keine.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen - SBL Betreff Blacklist*** aus.
2. Klicken Sie in der Listenansicht die rechte Maustaste.
3. Wählen Sie in der Auswahlliste den Eintrag **Neu**.
   Folgende Felder werden angezeigt:

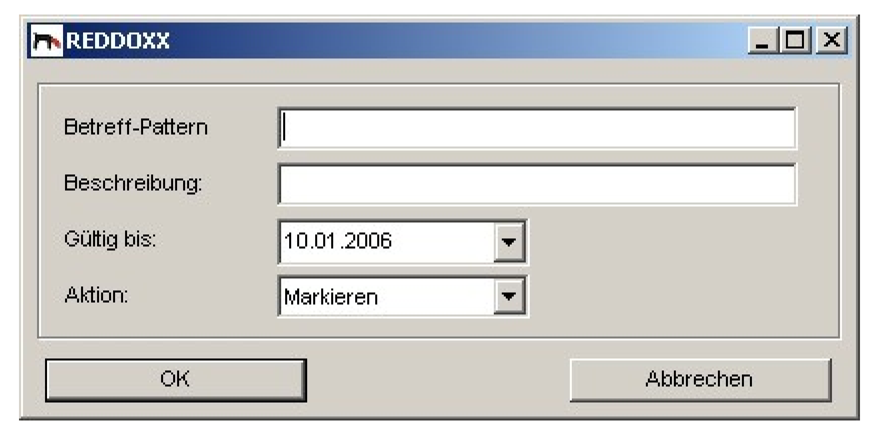



Abbildung: Sperren und Zulassen - SBL Betreff Blacklist

4. Geben Sie eine Zeichenfolge an.
5. Geben Sie an bis wann der Filter gültig sein soll.
   Die Vorbelegung lautet: Heute + 365 Tage
   Klicken Sie auf die Auswahlliste *Gültig bis*, wenn Sie einen Kalender zur Auswahl des Datums benötigen.

6. Wählen Sie über die Auswahlliste die *Aktion* für den Filter aus.
   Die Einstellungen Markieren, Quarantäne und Ablehnen sind möglich.
7. Kommentieren Sie den Filter bei Bedarf.
8. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

#### Filter bearbeiten

Um einen bereits bestehenden Filter zu bearbeiten, gehen Sie wie folgt vor.
**Voraussetzungen:** Filter in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen*** die jeweilige Filterliste aus.
2. Klicken Sie den zu bearbeitenden Filter doppelt an.
   Das Fenster für die Konfiguration öffnet sich.
3. Nehmen Sie alle gewünschten Änderungen vor.
4. Klicken Sie OK, um die Konfiguration zu speichern und zu schließen.
   ABBRECHEN: Änderungen verwerfen und Schließen der Konfiguration.

#### Filter löschen

Um einen bereits bestehenden Filter zu löschen, gehen Sie wie folgt vor.
**Voraussetzungen:** Filter in der Listenansicht vorhanden.

1. Wählen Sie in der Baumansicht unter ***Sperren und Zulassen*** die jeweilige Filterliste aus.
2. Klicken Sie den zu löschenden Filter mit der rechten Maustaste an.
3. Wählen Sie in der Auswahlliste den Eintrag **Löschen**.
4. Bestätigen Sie die Sicherheitsabfrage mit JA, um die Internetdomäne zu löschen.
   NEIN: Internetdomäne wird nicht gelöscht.

## 4.5 REDDOXX MailDepot

Das REDDOXX MailDepot besteht aus 4 Bereichen: die Archiv Konfiguration, die Archiv Policies, der MSX Agent und die Archiv-Liste.

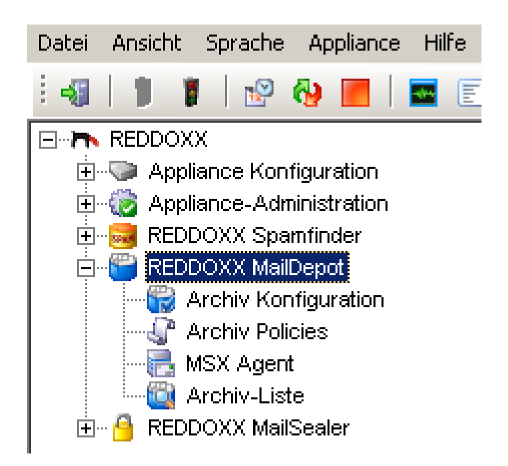



Abbildung: Navigationsbaum REDDOXX MailDepot

### 4.5.1 Archiv Konfiguration

#### 4.5.1.1 MailDepot - Allgemein

**Allgemeine MailDepot-Einstellungen vornehmen**

Über die Allgemeinen Einstellungen können Sie die E-Mail-Archivierung aktivieren, den Speicherort (=Archivtyp) auswählen, und den Zugriff auf eine Netzwerkfreigabe konfigurieren.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie in der Baumansicht auf ***REDDOXX MailDepot.***
2. Klicken Sie im Baum den Zweig ***Archiv Konfiguration*** doppelt an.
   Folgende Felder werden angezeigt:

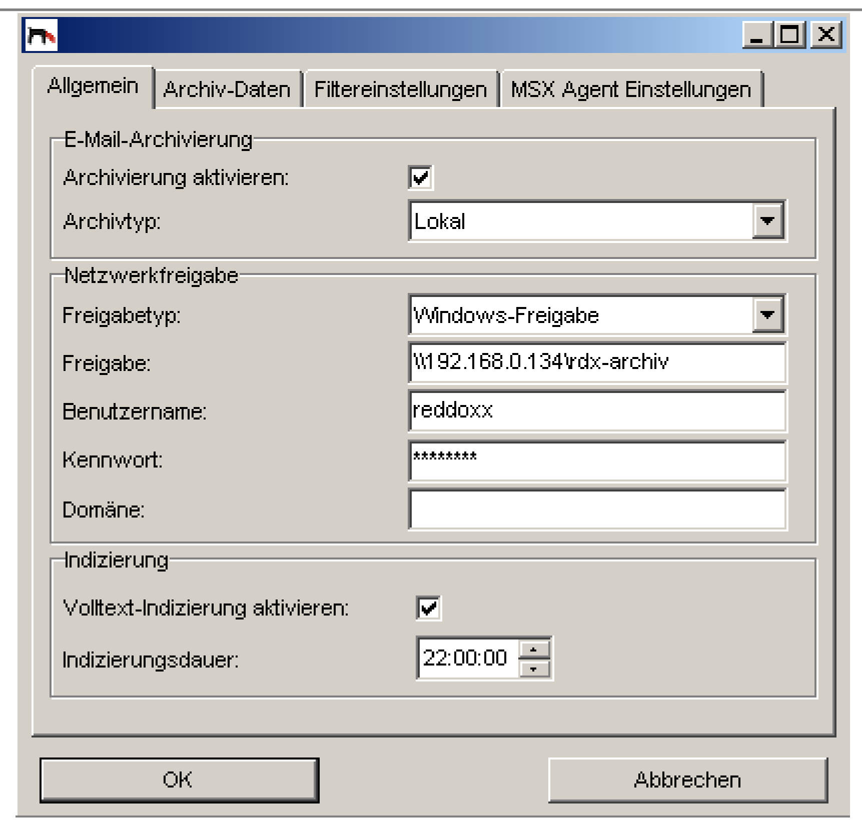



Abbildung: REDDOXX MailDepot Allgemein

3. *E-Mail-Archivierung - Archivierung aktivieren:*
   Schaltet die Archivierung ein oder aus.

**HINWEIS**

Ist die Archivierung aktiviert, werden standardmäßig alle ein- und ausgehenden E-Mails archiviert. Möglichkeiten, einzelne E-Mails von der Archivierung auszuschließen sind:

- Domänenweit (siehe lokale Internetdomänen-Konfiguation)
- pro E-Mailadresse (siehe E-Mail-Aliase-Konfiguration)
- Bei Spamerkennung (siehe Filtereinstellungen MailDepot)
- Durch Archiv Policies (siehe MailDepot)

4. *E-Mail-Archivierung - Archivtyp:*
   Der Archivtyp legt fest, ob die E-Mails lokal auf der REDDOXX Appliance oder auf einer Netzwerk Freigabe gespeichert werden.
5. *Netzwerkfreigabe - Freigabetyp:*
   Legt den Typ der Freigabe fest. Im Moment werden nur Windowsfreigaben unterstützt.
6. *Netzwerkfreigabe - Freigabe:* Geben Sie den UNC-Pfad ein

**HINWEIS**

Der Pfad wird im UNC (Uniform Naming Convention) im Format angegeben:
**\\servername\ordnername**

Bitte keine Unterverzeichnisse und abschließenden Backslash angeben!
Der Pfad für das MailDepot darf nicht derselbe sein, wie die Freigabe, die für das Backup konfiguriert wurde.

7. *Netzwerkfreigabe - Benutzername:*
   Geben Sie den *Benutzername* ein. Wir empfehlen aus Sicherheitsgründen, für die Archivierung nicht den Administrator, sondern einen separaten Benutzer auszuwählen (z.B. reddoxx)
8. *Netzwerkfreigabe - Kennwort:*
   Geben Sie das zugehörige *Kennwort* ein.
   **Das Kennwort darf nicht länger als 16 Zeichen sein!**
9. *Netzwerkfreigabe - Domäne:*
   Geben Sie eventuell den Namen der Domäne an, welcher zu der die Freigabe angehört.
10. *Volltextindizierung aktivieren:*
    Aktivieren Sie die Volltextindizierung, wenn Sie auf das Archiv mit der Volltextsuche zugreifen können wollen. Hierzu ist zuvor erforderlich, dass Sie denn Full Text Indexer in der Appliance Konsole einmal vollständig erstellt haben.
11. *Volltextindizierung aktivieren:*
    Indizierungsdauer (Zeitpunkt): Zeitpunkt, wann der Indexer täglich startet. Legen Sie die Startzeit so, dass der Indexer i.d.R. bereits fertig ist bevor das Backup startet.

    **HINWEIS**

    Der Indexer (Volltextindizierer) ist standardmäßig bereits aktiviert.
    Bedenken Sie, dass E-Mails erst nach dem täglichen Indizierungslauf über die Volltextsuche gefunden werden können.

12. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
    **OK**: Speichern und Schließen der Maildepot Konfiguration.
    **ABBRECHEN**: Änderungen verwerfen und Schließen der MailDepot Konfiguration.

### 4.5.1.2 MailDepot - Archiv-Daten

#### Archivdaten festlegen

Sie können die E-Mail-Archivierung von lokaler auf dezentrale Archivierung, oder umgekehrt, umstellen.
Der Datentransfer beginnt sofort nach dem Klicken auf einer der beiden Schaltflächen.
Beobachten Sie die Protokollanzeige auf evt. Fehlermeldungen.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Archiv-Daten".
   Folgende Felder werden angezeigt:

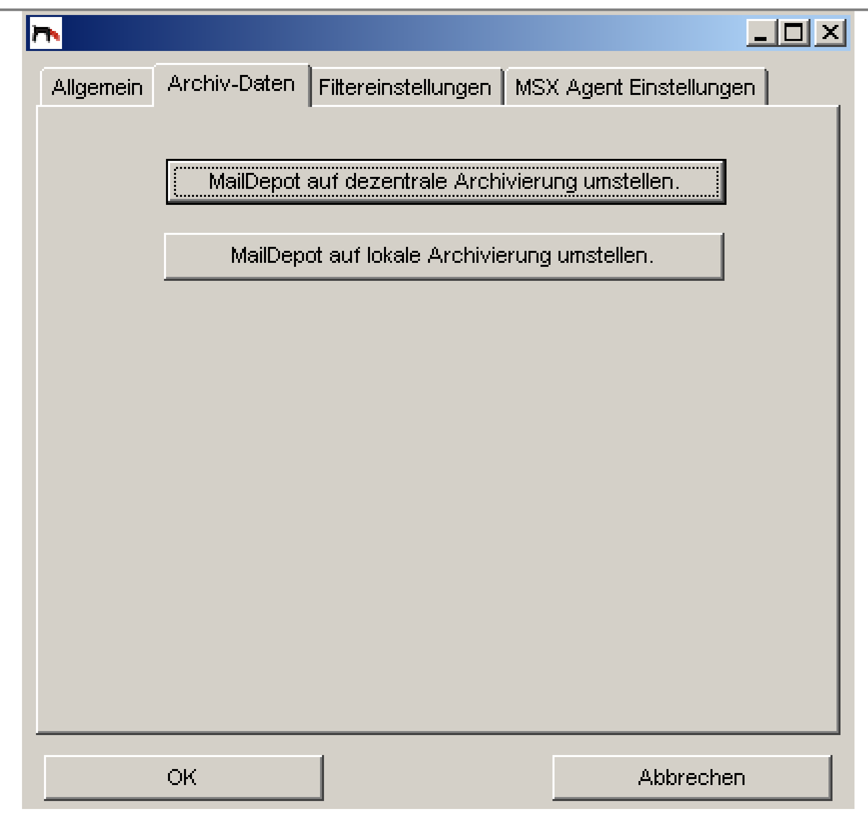



Abbildung: REDDOXX MailDepot Archiv-Daten

2. Button *MailDepot auf dezentrale Archivierung umstellen:*
   Die Archiv-Daten werden vom der lokalen Festplatte der REDDOXX Appliance in den UNC Pfad transferiert.
3. Button *MailDepot auf lokale Archivierung umstellen:*
   Die Archiv-Daten werden vom UNC Pfad auf die lokale Platte der REDDOXX Appliance transferiert.
4. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   OK: Speichern und Schließen der Maildepot Konfiguration.
   ABBRECHEN: Änderungen verwerfen und Schließen der Maildepot Konfiguration.

#### 4.5.1.3 MailDepot - Filtereinstellungen

**Filtereinstellungen festlegen**

Über die Filtereinstellungen können Sie den Archivierungs-Umfang definieren. Dabei kann festgelegt werden ob E-Mails, die von einem bestimmten Spamfilter als Spam deklariert sind, von der Archivierung ausgeschlossen werden.

**Voraussetzung:** Einstellungen öffnen.

1. Klicken Sie auf den Reiter "Filtereinstellungen".
   Folgende Felder werden angezeigt:

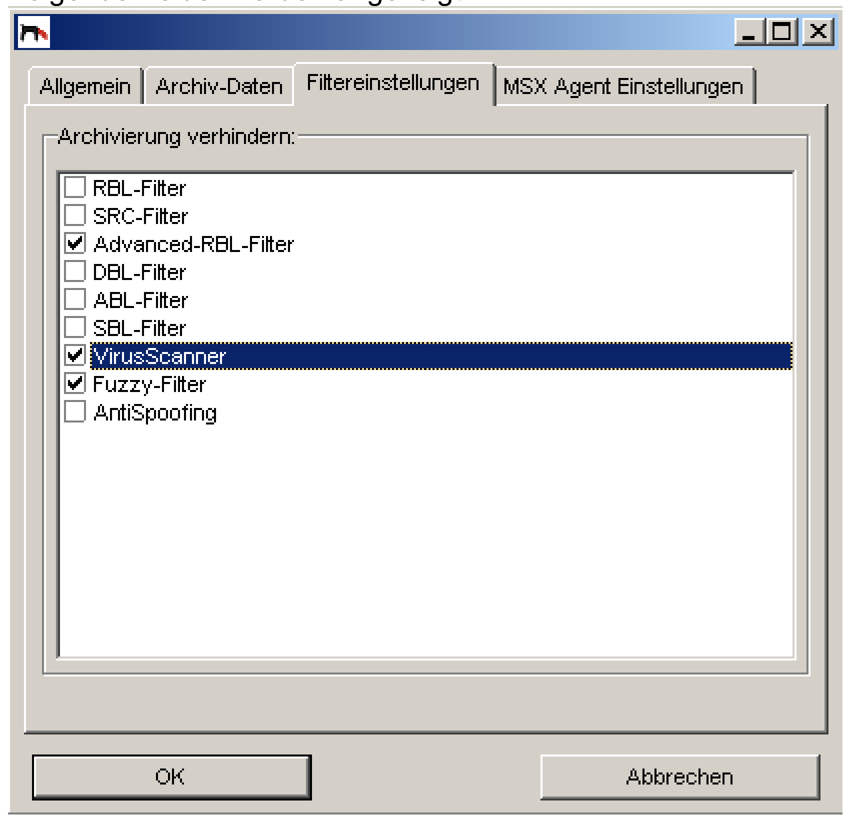



Abbildung: REDDOXX MailDepot Filtereinstellungen

2. **Archivierung verhindern:**
   Markieren Sie alle Filter, die eine Archivierung verhindern sollen.
3. Wechseln Sie für weitere Konfigurationen zum nächsten Reiter.
   **OK**: Speichern und Schließen der Maildepot Konfiguration.
   **ABBRECHEN**: Änderungen verwerfen und Schließen der Maildepot Konfiguration.

#### 4.5.1.4 MailDepot Microsoft Exchange Einstellungen

1. Klicken Sie auf den Reiter "Microsoft Exchange Einstellungen"
   Folgende Felder werden angezeigt:

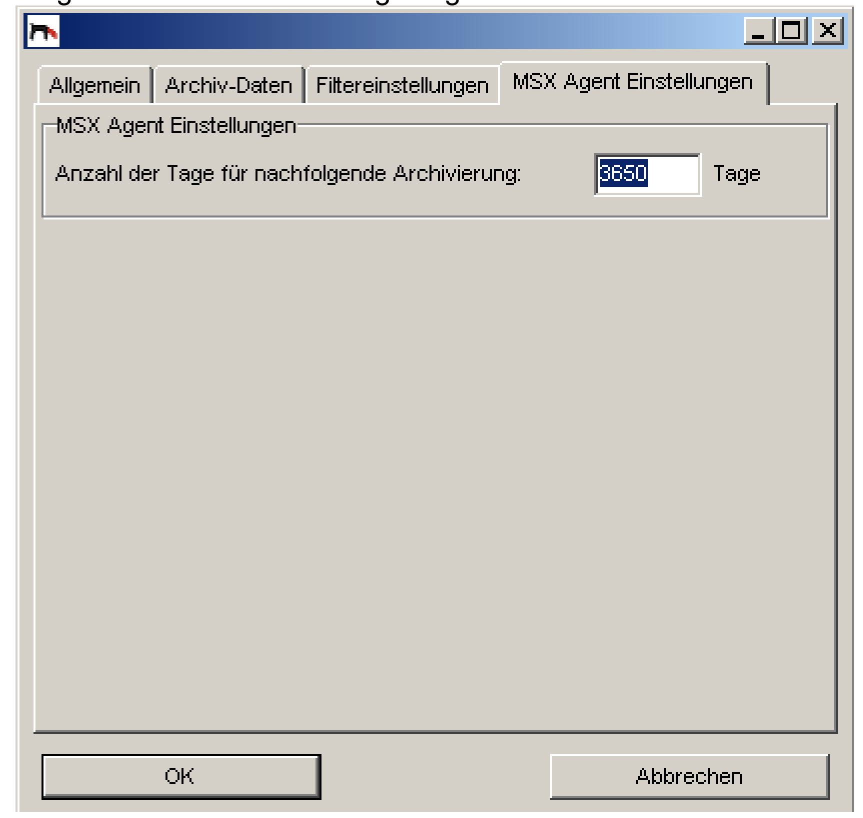



Abbildung: REDDOXX MailDepot Microsoft Exchange Einstellungen

2. **Anzahl der Tage für nachträgliches archivieren**:
   Dieser Wert bestimmt bei einer Nacharchivierung, um wie viele Tage zurück E-Mails nachträglich archiviert werden. Der Standardwert ist 3650 Tage. Es werden also bei einer Nacharchivierung alle E-Mails eines Postfaches der letzten 10 Jahre archiviert.
3. Klick auf OK: Der Dialog wird beendet. Änderungen sind sofort wirksam.

### 4.5.2 Archiv Policies

Mit den Archiv Policies kann man bestimmen, welche E-Mails archiviert - und welche nicht archiviert werden. Aus verschiedenen Gründen kann es gewünscht sein, dass bestimmte E-Mails nicht archiviert werden sollen. Ist das Archiv generell aktiviert, werden standardmäßig alle E-Mails archiviert. Mit einer Policy können Sie verhindern, dass E-Mails, die mit einem definierten Muster der Betreffzeile, des Absenders oder des Empfängers übereinstimmen, archiviert werden.

1. Klicken Sie im Navigationsbaum auf **Archiv Policies.**

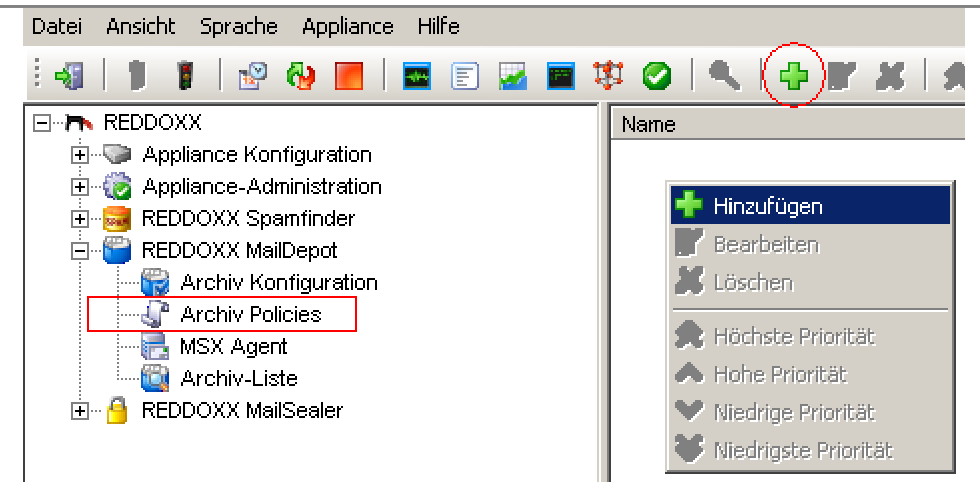



Abbildung: Hinzufügen einer Policy

2. Klicken Sie auf das grüne Plus-Symbol oder klicken Sie rechts im Listenbereich und wählen Sie **HINZUFÜGEN** aus dem Kontextmenü.
   Folgende Felder werden angezeigt:

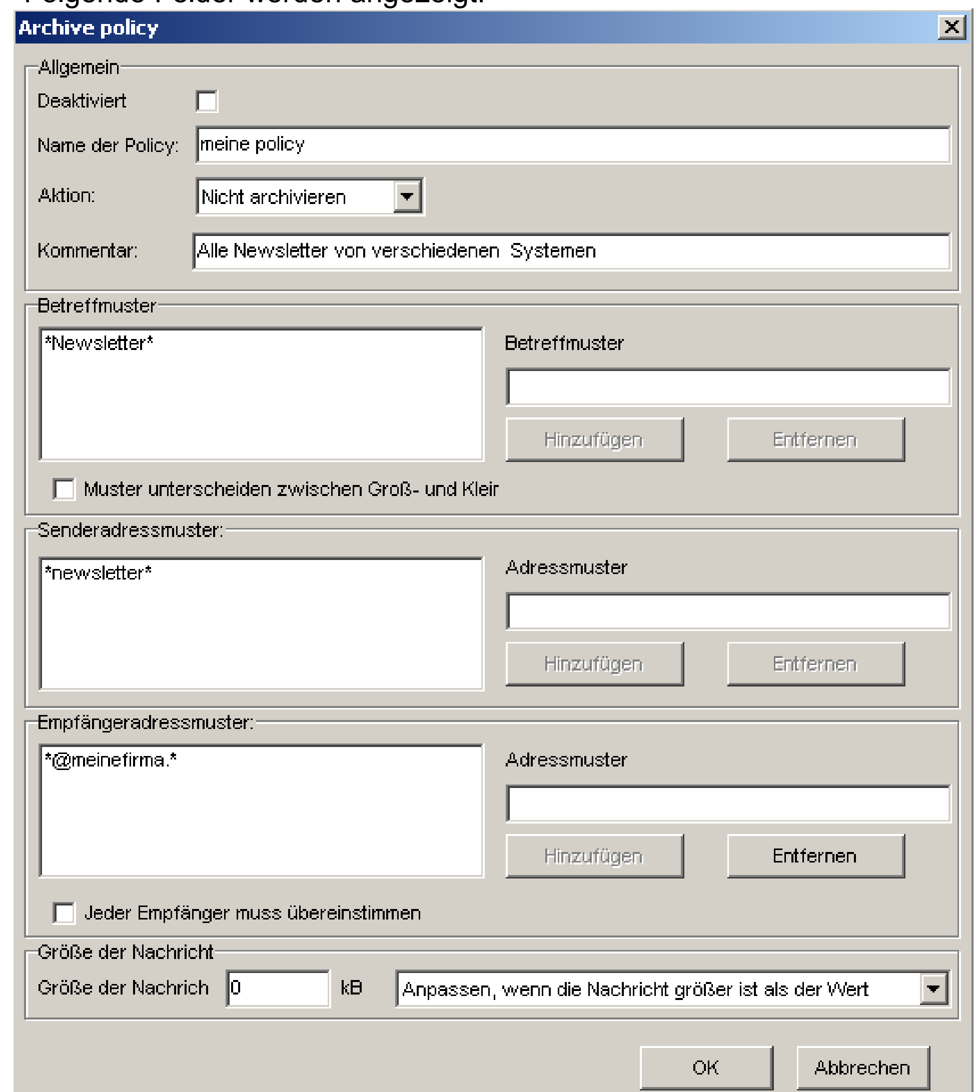



Abbildung: Policy hinzufügen

1. **Deaktiviert**:
   Aktivieren Sie diese Checkbox, wenn Sie kurzzeitig diese Policy deaktivieren wollen.

2. **Policy Name**:
   Der Name dieser Archiv Policy.

3. **Aktion**:
   Wählen Sie zwischen **archivieren** und **Nicht archivieren**. Sie können verschiedene Policies kombinieren. Setzen Sie alle Policies in eine gewünschte Reihenfolge, beginnend von oben nach unten. Sie können die Reihenfolge einer Policy durch die blauen Pfeile verändern. 

**HINWEIS**

Um generell die Archivierung zu unterbinden, setzen Sie eine Policy ans Ende der Liste. Definieren Sie Policies mit den Ausnahmen, die Sie dennoch Archivieren wollen vor der letzten Policy. Die Abarbeitungsreihenfolge der Policies geht von oben nach unten. Wenn die Bedingungen einer Policy auf eine bestimmte E-Mail zutreffen, endet die Abarbeitung der Policies an diese Stelle.

4. **Kommentar**:
   Ein Kommentar beschreibt die Policy.

5. **Betreffmuster**:
   Geben Sie hier das Muster ein, das mit der Betreffzeile der E-Mail übereinstimmen soll. Verwenden Sie einen Stern (*), um generische Vergleiche zu ermöglichen.
   Beispiel: ***Newsletter*.** Das bedeutet, dass “**1stNewsletter-2008**” auch zutrifft.

6. **Groß-/Kleinschreibung berücksichtigen**
   Ist die Checkbox aktiviert, wird die Groß-/Kleinschreibung des Betreffsmusters berücksichtigt.

7. **Absenderadressmuster**:
   Beispiel: ***newsletter*** . Das trifft auf alle E-Mails zu, die in der Mailboxadresse oder im Domänennamen das Wort „newsletter“ haben.

8. **Empfängeradressmuster**:
   Beispiel: ***@meinefirma.*** **.** Dies trifft auf alle Empfänger zu, die im Domänennamen “meinefirma” beinhaltet, egal welcher TLD (top level domain) sie angehört.

9. **Jeder Empfänger muss adressiert sein**:
   Ist diese Checkbox gesetzt, gilt: Nur wenn eine E-Mail an alle Empfänger dieser Liste adressiert wurde, wird diese Policy angewendet.

10. **Größe der Nachricht:**
    Geben Sie die gewünschte Größe ein und wählen Sie die dafür entsprechende Aktion aus. Wählen Sie zwischen ***Anwenden, wenn die Nachricht größer ist als der Wert*** und **Anwenden, wenn die Nachricht kleiner ist als der Wert*.***

11. Klicken Sie **OK** um die Änderungen zu speichern.

**HINWEIS**

Die nachfolgenden Felder stehen in Kombination zueinander und werden mit einem logischen **UND** verknüpft. In anderen Worten: Nur wenn alle Bedingungen zutreffen, wird die definierte Aktion ausgeführt (archivieren oder nicht archivieren).
**Betreffmuster, Absendermuster, Empfängermuster, Nachrichtengröße.**

## 4.5.3 Exchange Server Agents

### 4.5.3.1 Hinzufügen eines neuen MSX Agenten

1. Klicken Sie im Navigationsbaum auf **MSX Agenten.**

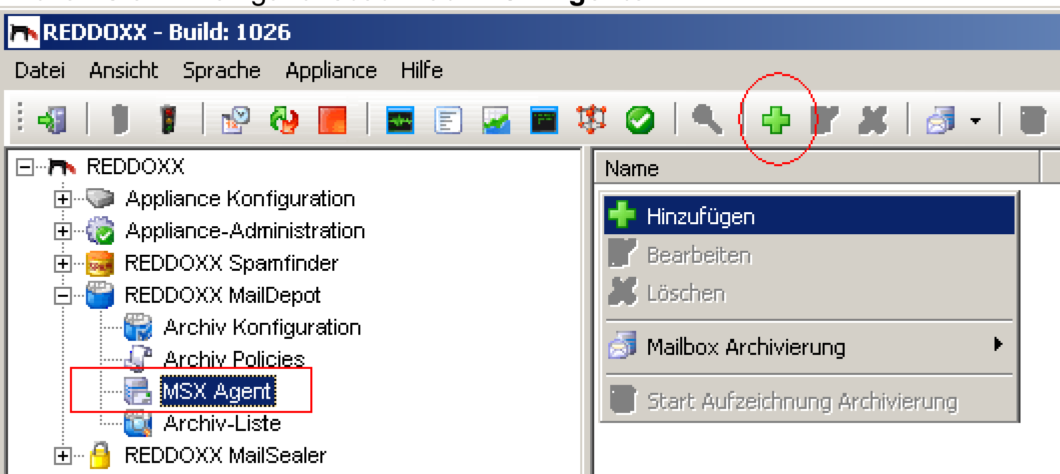



Abbildung: Einen neuen MSX-Agenten hinzufügen

2. Klicken Sie auf das grüne Plus-Symbol oder klicken Sie rechts in den Listenbereich und wählen Sie HINZUFÜGEN aus dem Kontextmenü.
Der folgende Dialog öffnet sich:




Abbildung: MSX Agent Einstellungen

3. **Hostname**:
Enter the hostname or IP Address of the MS Exchange Server.

4. **Port**:
Auf diesem TCP-Port lauscht der MSX-Agent auf dem Exchange Server und erwartet die Kommandos zum Archivieren von der REDDOXX Appliance. Der Standardwert ist: 4088.

5. **Archivierungsinterval**:
Die Zeitdauer, wann wieder E-Mails vom MS Exchange Server abgeholt werden. Der Standard ist: 60 Minuten.

6. Klicken Sie auf **OK.**
Sofern Sie eine IP Adresse eingegeben haben, wird diese in den Hostnamen des Exchange Servers umgewandelt.




## 4.5.3.2 Mailbox Archivierung

Mit der Mailbox Archivierung können Sie ganze Mailboxen (Postfächer) nacharchivieren. Mit der Journaling Mailbox Funktion (siehe nächstes Kapitel 4.5.3.3) werden neue E-Mails zyklisch archiviert. E-Mails vor der Aktivierung des Journals werden dabei nicht berücksichtigt. Diese alten E-Mails können Sie über die Mailbox Archivierung jederzeit nacharchivieren. Mögliche Duplikate mit neuen E-Mails werden dabei von der Appliance berücksichtigt.

1. Klicken Sie im Navigationsbaum auf **MSX Agenten.**
2. Klicken Sie rechts auf einen gelisteten Exchange Server.
   Das folgende Kontextmenü wird angezeigt:

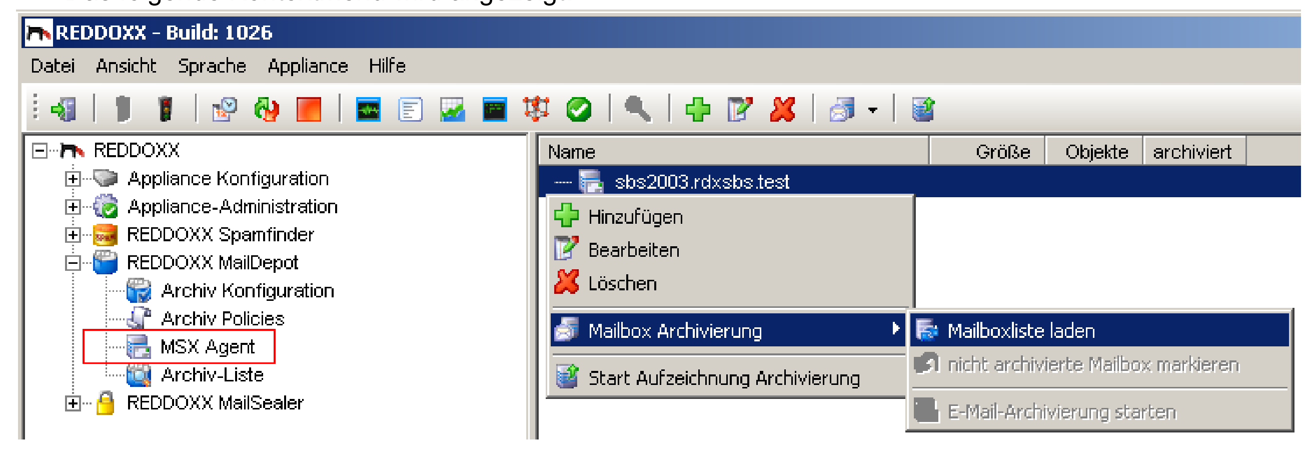



Abbildung: Mailbox Archivierung – Mailboxliste laden

3. Wählen Sie **Mailbox Archivierung.**
4. Wählen Sie **Mailboxliste laden**.
   Eine Liste der Mailboxen angezeigt:

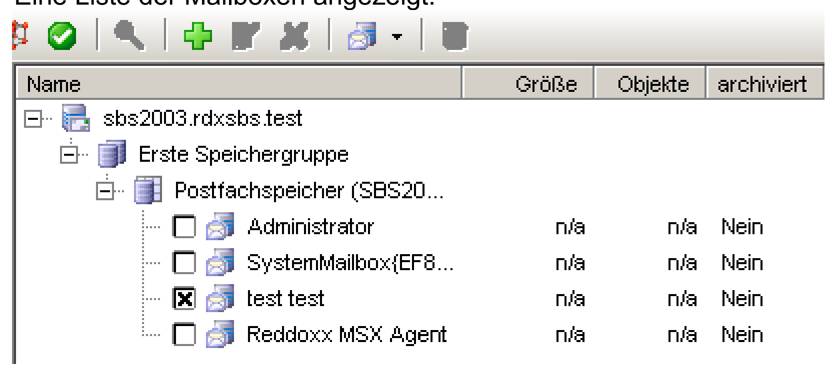



Abbildung: Liste von Mailboxen zum Nacharchivieren

5. Aktivieren Sie die Checkbox der Mailboxen, die Sie nacharchivieren möchten.
6. Klicken Sie rechts auf einer der ausgewählten Mailboxen.
   Das folgende Kontextmenü wird angezeigt:

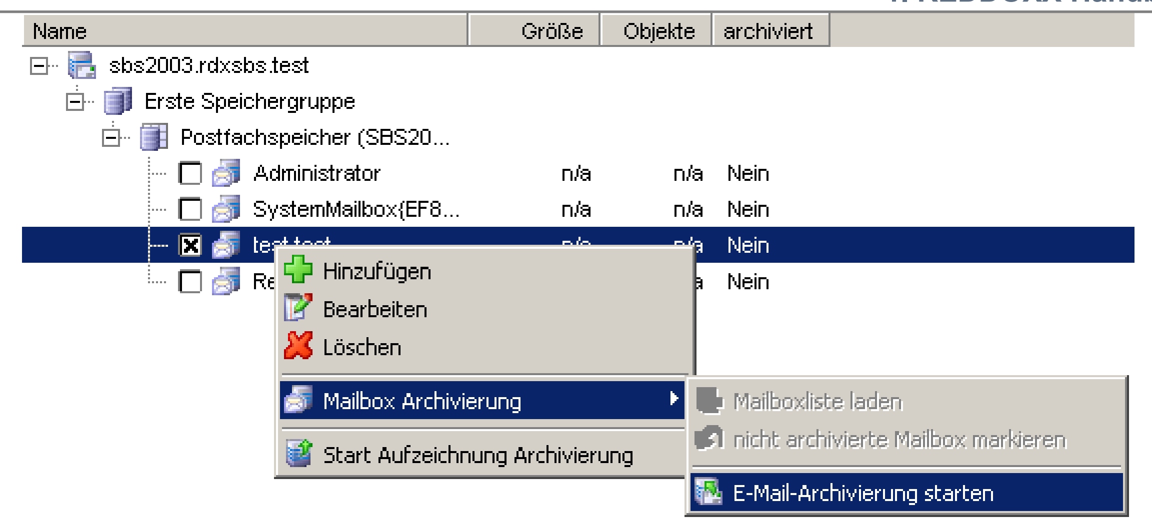
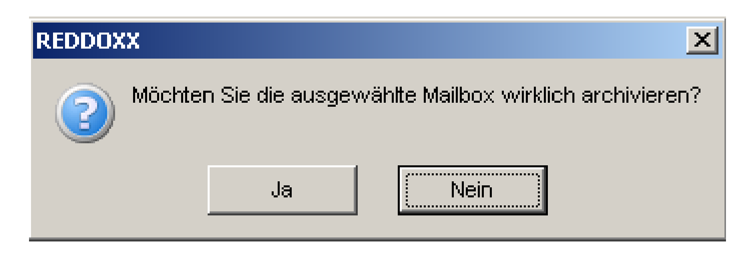



Abbildung: Mailbox Archivierung starten

7. Wählen Sie **Mailbox Archivierung**, dann **E-Mail Archivierung starten**. Bestätigen Sie den nachfolgenden Dialog mit **JA**.




Der Archivierungsprozess startet nun. Sie können die einzelnen Schritte im Protokollfenster verfolgen und prüfen, ob die einzelnen E-Mails ordnungsgemäß archiviert werden. Nachfolgend eine beispielhafte Abbildung.

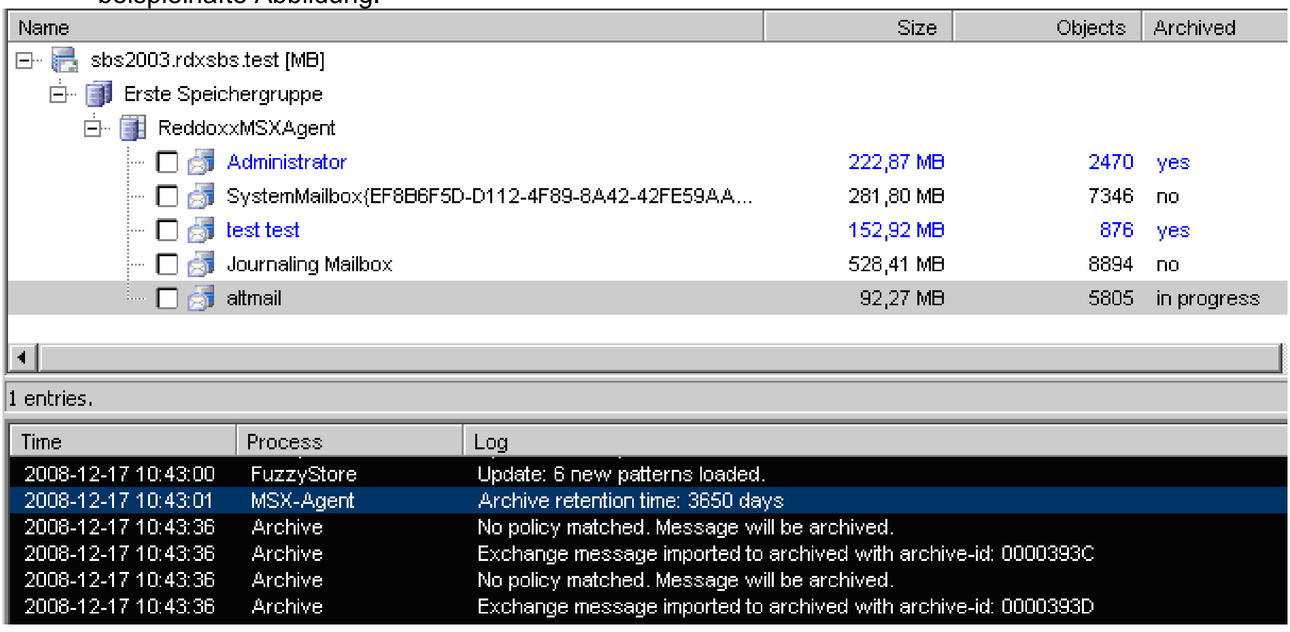



Abbildung: Protokollfenster während einer Archivierung

### 4.5.3.3 Journaling Mailbox Archivierung

Mit der Journaling Mailbox Archivierung werden interne E-Mails regelmäßig archiviert. Der Standardwert liegt bei 60 Minuten. Sie können den Wert in der Archiv-Konfiguration ändern. Sie können aber auch das journalbasierte Archivieren sofort anstoßen.

1. Klicken Sie rechts auf einen gelisteten Hostnamen eines MS Exchange Servers.
   Das folgende Kontextmenü erscheint:

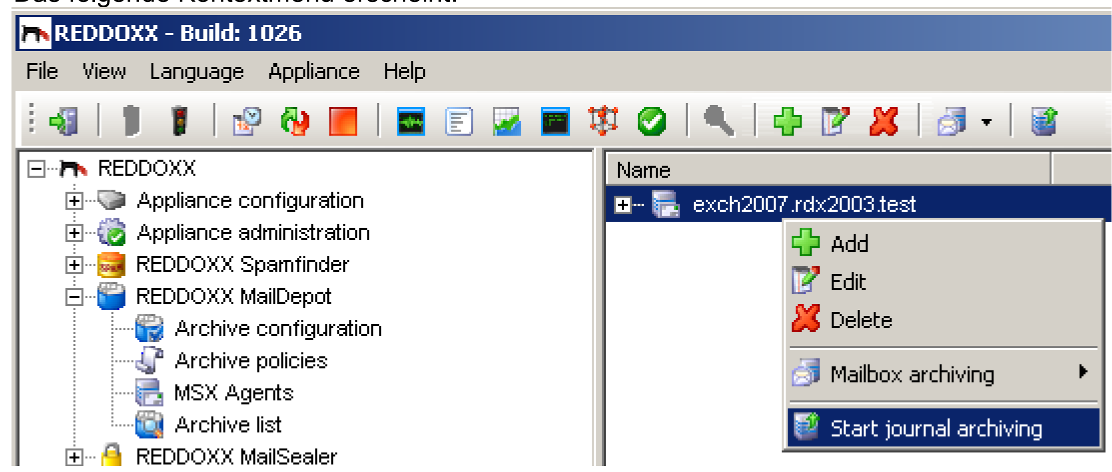



Abbildung: Start journal archiving

2. Wählen Sie **Start journal archiving.**
   Eine Bestätigung des Starts wird angezeigt. Klicken Sie OK.




Abbildung: Journal Archiving Started

3. Überprüfen Sie das Archivieren im Protokollfenster.

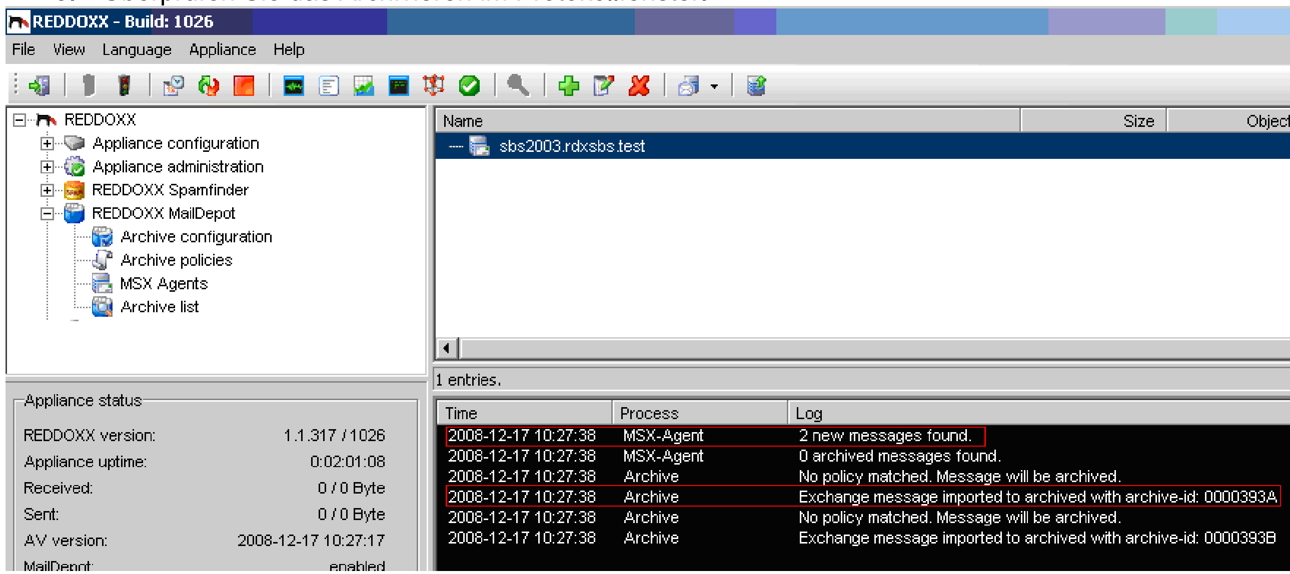



Abbildung: Journaling Mailbox Archiving Protocol

### 4.5.4 Archiv-Liste

**Die MailDepot Archiv-Liste**

In der Archiv-Liste sehen Sie alle vom MailDepot archivierten E-Mails, mit Ausnahme der Spam- (inkl. CISS) und Viren-E-Mails. Diese können Sie anzeigen lassen, indem Sie die jeweiligen Checkboxen bei der *Erweiterten Suche* aktivieren.
Die Ergebnisliste wird zuerst auf 1000 Einträge beschränkt. Sie können sich alle Einträge anzeigen lassen, indem Sie im Suchfeld ein „@" eingeben und die Suche starten. Bedenken Sie dabei, dass die Suche sehr lange dauern kann, entsprechend der Anzahl Einträge in Ihrem Maildepot.
Des Weiteren können Sie die Anzeige auch durch die Einstellungswerte des Anzeigezeitraums unter APPLIANCE ADMINISTRATION – EINSTELLUNGEN – ERWEITERT (siehe Kapitel 4.1.2.4) begrenzen.

**Voraussetzung:** MailDepot ist aktiv.

Klicken Sie im Navigationsbaum auf **Archiv-Liste**
Folgende Ansicht wird angezeigt:




Abbildung: REDDOXX MailDepot Archiv-Liste

**Die folgenden Felder werden in der Liste angezeigt:**

1. **Status**: (Der Titel wird nicht angezeigt)
   Regulär archivierte E-Mail.
   Als Virus erkannte E-Mail, archiviert.
   Als Spam erkannte E-Mail, archiviert.
2. **ID**:
   Eine eindeutige Archiv-ID unter welcher diese E-Mail im System referenziert ist.
3. **Mailfluss Richtung**: (Der Titel wird nicht angezeigt)
   Ausgehende Nachricht.
   Eingehende Nachricht.
   Outlook-Nachricht, die nacharchiviert wurde.
4. **Zeit der Nachricht**:
   Datum und Uhrzeit der E-Mai, als sie erstellt wurde. Interne E-Mails, die mit Outlook erstellt wurden, zeigen das Datum, an dem der Benutzer die Nachricht versendet hatte.
5. **Betreff**:
   Der Betreff der Nachricht.
6. **Absender**:
   Der Absender der Nachricht.
7. **Empfänger**:
   Der Empfänger der Nachricht.
8. **Größe**:
   Die Größe der Nachricht.
9. **Anhänge**:
   Dateinamen des E-Mail-Anhanges.
10. **MS**:
   Wenn das Symbol in dieser Spalte angezeigt wird, wurde diese Nachricht

kryptografisch verarbeitet. Das bedeutet, dass die E-Mail entweder verschlüsselt oder signiert oder beides wurde.

11. **Archiv-Zeit**:
    Die Zeit, an der die E-Mail archiviert wurde. Dieser Wert kann stark vom E-Mail-Erstellungsdatum abweichen, beispielweise durch den Journaling Mailbox Archivierungsdienst, der standardmäßig alle 60 Minuten startet.

**Suchfelder:**

12. **Suchbegriff**:
    Geben Sie das Kriterium ein, nachdem Sie suchen möchten.
13. **Suche in:**
    Wählen Sie das gewünschte Feld aus der Liste. Die Vorbelegung ist "*Absender und Empfänger". A*ndere Auswahlmöglichkeiten sind: *Betreff, Absender, Empfänger, Anhänge*.
14. **Suche**:
    Klicken Sie auf **Suche** um die *Standard Suche* zu starten.
15. **Erweitert**:
    Klicken Sie auf *ERWEITERT* um die Erweiterte Suche zu öffnen.
    Das folgende Fenster öffnet sich:

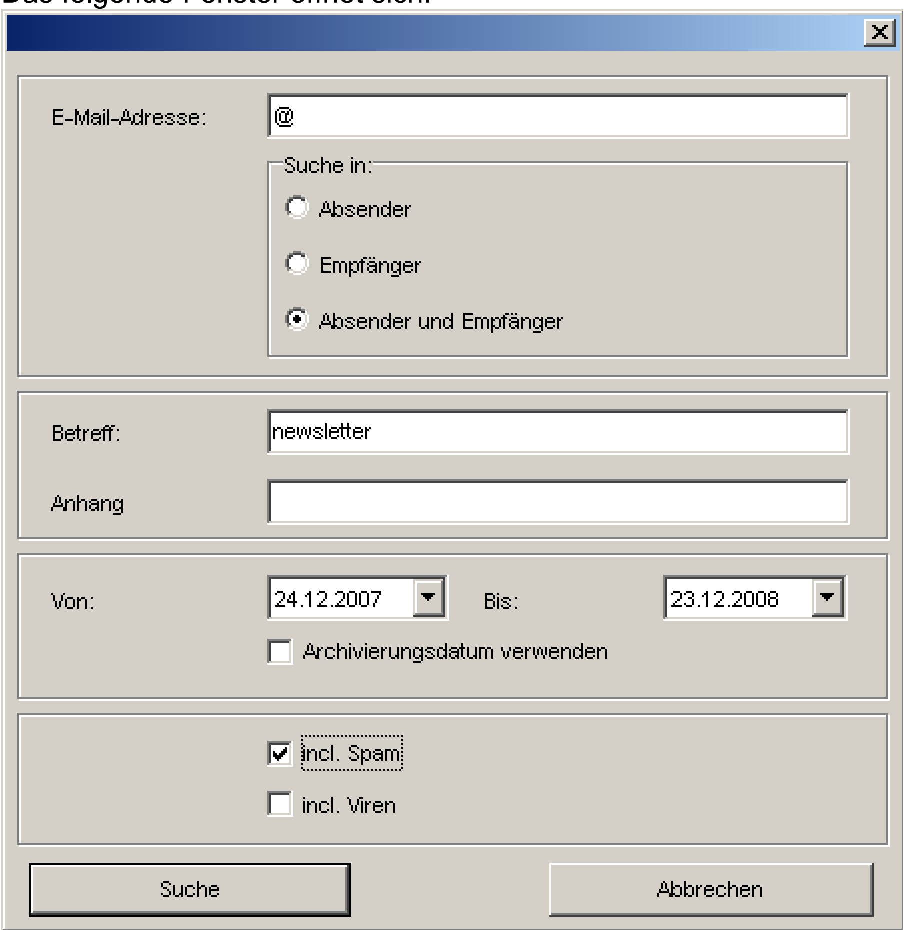



Abbildung: REDDOXX MailDepot Archiv-Liste – Erweiterte Suche

16. **E-Mail-Adresse:**
    Geben Sie eine E-Mail-Adresse ein, nach der Sie suchen möchten. Ein “@” at-Zeichen steht für: Alle E-Mails.
17. **Suche in:**
    Wählen Sie den gewünschten Feldtyp aus. Der Standard ist *"Absender und Empfänger".* Weitere Auswahlmöglichkeiten sind: *Absender* oder *Empfänger.*

18. **Betreff:**
    Sucht nach einen vorgegebenen Muster in der Betreffszeile. Die Groß-Kleinschreibung wird dabei nicht berücksichtigt, d.h. es gilt: sowohl als auch.
19. **Anhang**:
    Sucht nach dem Dateinamen im Anhang der Nachricht.
20. **Bis**:
    Sucht bis zu diesem Zeitpunkt (Erstellungsdatum der Nachricht).
21. **Von:**
    Sucht ab diesem Zeitpunkt (Erstellungsdatum der Nachricht).
22. **Archivierungsdatum verwenden:**
    Anstelle des Erstellungsdatums wird bei der Suche das Archivierungsdatum verglichen.
23. **Incl. Spam:**
    Aktivieren Sie die Checkbox, damit auch als Spam erkannte E-Mails gefunden werden. Dies gilt insbesondere auch für CISS-Challenges.
24. **Incl. Viren:**
    Aktivieren Sie die Checkbox, damit auch als Viren erkannte E-Mails gefunden werden.
25. **Klicken Sie auf SUCHE**:
    Die Suche kann, abhängig der Größe des Archivs und Ihren Such-Kriterien einen Moment oder eine Weile dauern.

**HINWEIS**

Auch E-Mails, die in der CISS-Warteschlange gelandet sind, wurden bereits archiviert. Unabhängig davon, ob die Challenge beantwortet, oder die E-Mail aus der Warteschlange zugestellt wurde. Um sie zu finden, müssen Sie in der Erweiterten Suche das Feld „**Incl. Spam**“ aktivieren.

## 4.6 REDDOXX MailSealer

**Einleitung**

Mit dem MailSealer können Sie E-Mails für den Versand signieren und verschlüsseln. Dabei können Sie zwischen verschiedenen Methoden wählen, die in 2 Produktgruppen aufgeteilt sind.
Der ***MailSealer Light*** verschlüsselt auf Basis einer Passphrase (symmetrisch). Der ***MailSealer*** verschlüsselt und signiert nach S/MIME oder PGP auf der Basis von X509v3-Zertifikaten bzw. Schlüsselpaaren (asymmetrisch).

### 4.6.1 Ad-Hoc Verschlüsselung mit dem MailSealer Light

Für eine schnelle und einfache Verschlüsselung mit einer Passphrase innerhalb der Betreffzeile ohne Konfigurationsaufwand.
Um einmalig eine E-Mail verschlüsselt zu versenden, geben Sie in der Betreffzeile Ihre Passphrase ein. Die Passphrase wird durch zuvor definierte Zeichen eingegrenzt. Der Default lautet (*….*).

Anwendungs-Beispiel:

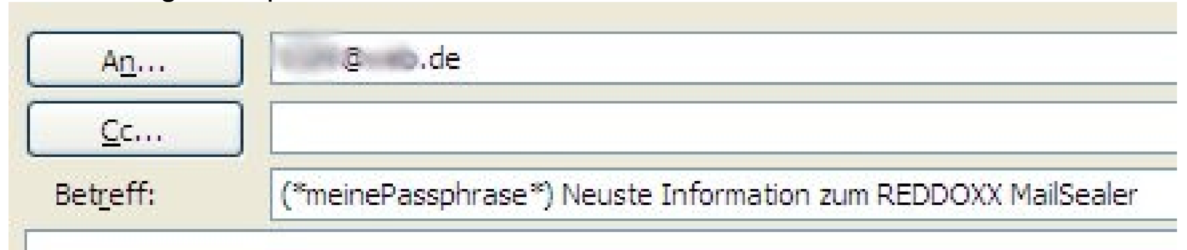



Abbildung: Betreff mit Angabe einer Passphrase zur Ad-hoc-Verschlüsselung mit MailSealer Light

Mit dem Absenden gelangt die E-Mail zuerst zur eigenen REDDOXX, wo sie anhand der Passphrase verschlüsselt wird. Die Passphrase wird dabei aus der Betreffzeile entfernt und der Text *MailSealer**:*** dem Betreff vorangestellt. Danach wird die E-Mail zugestellt. Im Nachrichten-Text erscheint beim Empfänger folgender Hinweis.

Von: info@exmall24.net Gesendet: So 13.05.2007 12:34
An:
Cc:
Betreff: MailSealer: neue Information zum REDDOX MailSealer

Anlagen: message.rdxmsl (789 B)

?REDDOXX-MailSealer

Der Absender hat diese Mail mit dem REDDOXX-MailSealer light verschlüsselt, da Sie vertrauliche Informationen enthält.

Um die Mail zu lesen benötigen Sie den kostenlosen REDDOXX-MailSealer light Reader den Sie hier downloaden können.

Url: http://mailsealer.reddoxx.net

Die benötigte Verschlüsselungs-Passphrase erhalten sie vom Absender.

Abbildung: E-Mail-Hinweis auf eine verschlüsselte Nachricht

Die verschlüsselte E-Mail ist als Attachment *„message.rdxmsl“* angehängt. Beim Doppelklick auf den Anhang öffnet sich der Reader und verlangt die Passphrase.

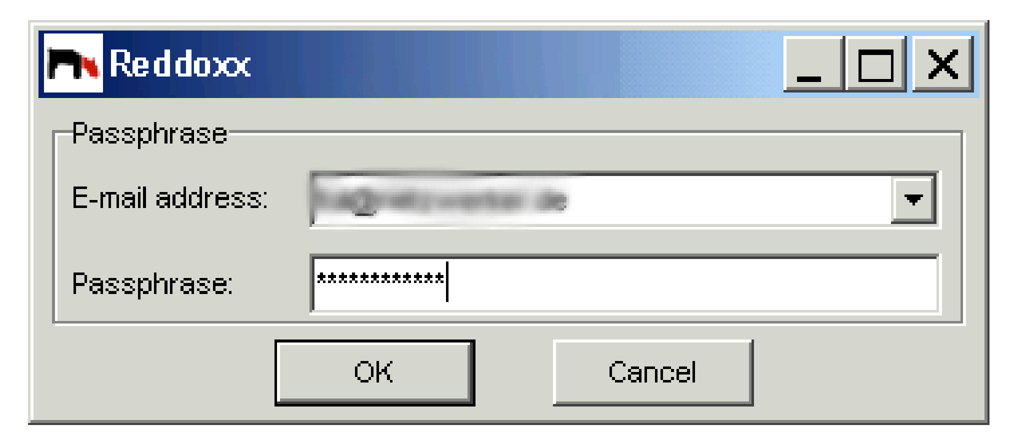



Abbildung: MailSealer light Reader: Eingabe der Passphrase

Nach erfolgreicher Eingabe zeigt der Reader die verschlüsselte E-Mail im Klartext an.

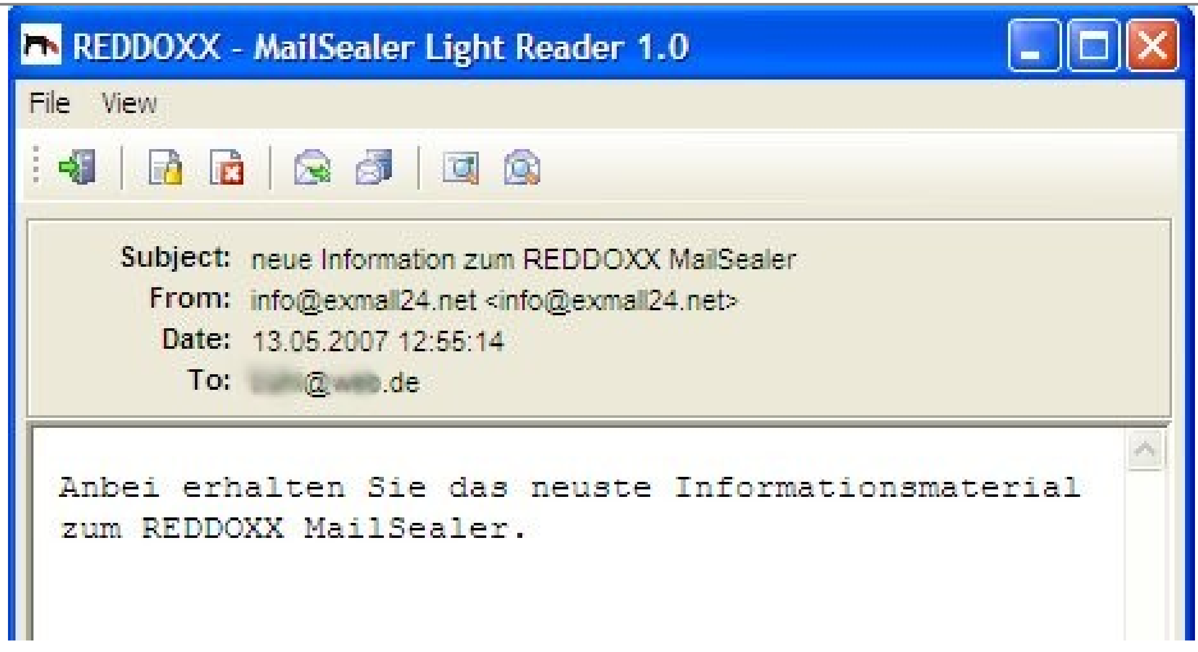



Abbildung: Ansicht einer entschlüsselten E-Mail im MailSealer Light-Reader

**HINWEIS**

Erhält der Empfänger zum ersten Mal eine verschlüsselte E-Mail von einer REDDOXX, so muss er einmalig den MailSealerLight-READER vom angegebenen Hyperlink herunterladen und dieses Programm mit der Dateiendung .rdxmsl verknüpfen.

## 4.6.2 Permanente Verschlüsselung mit dem MailSealer Light

Bei der permanenten Verschlüsselung hinterlegt der Benutzer in der User-Konsole die Passphrase für jede E-Mail-Adresse, an die er verschlüsselt senden möchte. Die Zustellung erfolgt dann wie bei der Ad-Hoc Methode.

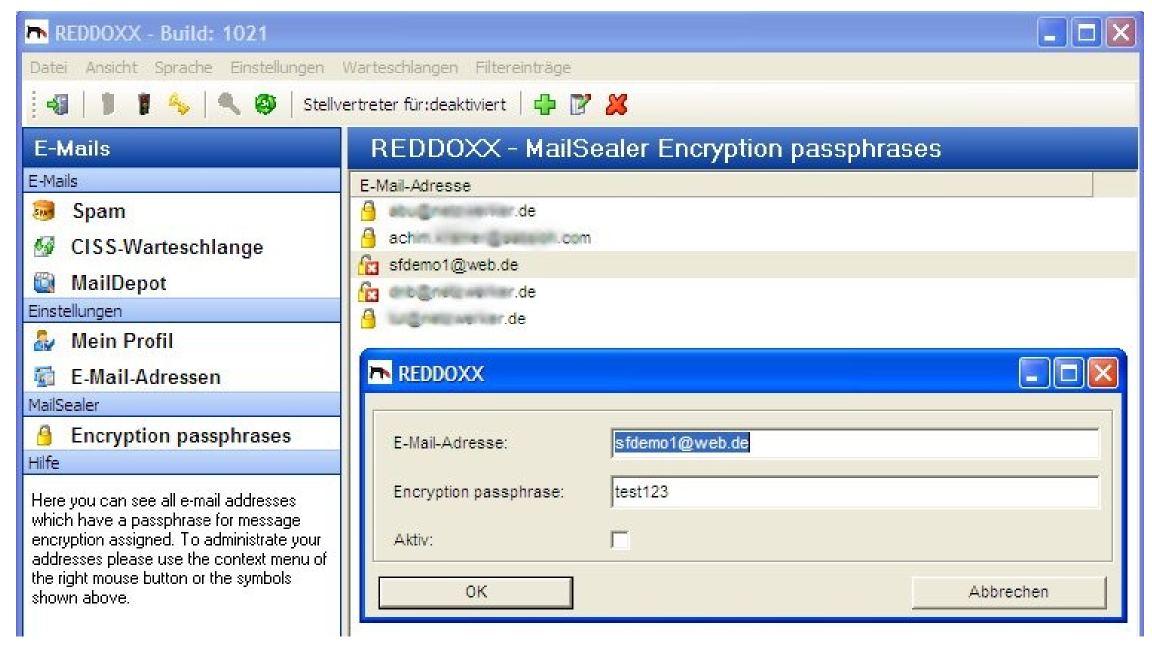



Abbildung: Passphrase-Einstellung in der User-Konsole

## 4.6.3 MailSealer Light-Gateways

Automatische Ver- und Entschlüsselung von E-Mails auf Basis von Passphrases. Verfügt der Empfänger ebenfalls über eine REDDOXX Appliance, so kann er die Passphrase zum Entschlüsseln der E-Mail in der Benutzerkonsole hinterlegen. Die E-Mail wird bei Eingang automatisch entschlüsselt und dem Postfach zugestellt. Dieser Vorgang erfolgt völlig transparent und benötigt keinen weiteren Eingriff seitens der Benutzer.

## 4.6.4 Asymmetrische Verschlüsselung mit PGP-Keys und S/MIME

Die asymmetrische Verschlüsselung benutzt das sogenannte Public-Key-Verfahren. Jeder Benutzer (Versender) besitzt ein eigenes, ihm eindeutig zuordenbares Schlüsselpaar aus einem ***Private Key*** (privater Schlüssel) und einem ***Public Key*** (öffentlicher Schlüssel).

Die Nachrichten an den Empfänger werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können dann ausschließlich vom Empfänger selbst mit seinem privaten Schlüssel entschlüsselt werden. Dabei ist es Voraussetzung, dass vor der ersten Verschlüsselung die Public Keys untereinander ausgetauscht wurden. Dies erfolgt üblicherweise durch den Versand einer signierten E-Mail. Wann eine E-Mail signiert oder auch verschlüsselt wird, wird durch die Policies der REDDOXX Appliance bestimmt.

### 4.6.5 Verschlüsselung mit PGP-Keys

Beim PGP-Verfahren kann der Versender sich sein PGP-Schlüsselpaar selbst erstellen oder aber er bekommt es durch eine unternehmensweite Public Key Infrastructure (PKI) zugewiesen.
Das PGP-Verfahren (Pretty Good Privacy) wird jedoch derzeit von der REDDOXX Appliance noch nicht unterstützt. Benutzen Sie anstelle dessen das S/MIME Verfahren (siehe nachfolgend).

### 4.6.6 Verschlüsselung mit S/MIME Zertifikaten

Durch ein Zertifikat wird beglaubigt, dass der Absender einer E-Mail (Absenderadresse im Header der E-Mail) mit der E-Mailadresse des Zertifikates übereinstimmt.
S/MIME-Zertifikate (X.509v.3) sind üblicherweise personenbezogen und werden durch eine vertrauenswürdige Zertifizierungsstelle (***Certificate Authority, kurz CA***) ausgestellt. Zertifikate können bei kommerziellen Anbietern erworben werden (z.B.: VeriSign, Thawte, CaCert etc.). Nach dem Erhalt des Zertifikates muss dieses auf der REDDOXX-Appliance in den privaten Zertifikatsspeicher importiert werden.
Sie können aber auch Zertifikate für Ihre Anwender durch Ihre REDDOXX Appliance automatisch erstellen lassen, indem Sie ein eigenes, sog. selbst-signiertes (engl: self signed) Root-CA Zertifikat erstellen. Der E-Mail-Partner vertraut Ihnen dann dadurch, dass er Ihr selbstsigniertes Root-Zertifikat in seinen Zertifikatsspeicher für Autoritäten (Certificate Authorities) importiert.

### 4.6.7 Verschlüsselung mit Gateway-Zertifikaten (S/MIME)

Bei den S/MIME ***Gateway***-Zertifkaten (auch ***company***- oder ***Domain***-Zertifikate genannt) wird die E-Mail auf einem Gateway (in diesem Fall die REDDOXX Appliance) für alle Benutzer dieser Domäne mit einem einzigen Zertifikat verschlüsselt. Auf der Gegenstelle (Empfangsseite) wird dabei nur die Absenderdomäne des Zertifikates mit der eigentlichen Absenderdomäne der E-Mail verglichen und somit dem Absender bei Übereinstimmung vertraut. Der Vorteil dabei ist, dass nur ein Zertifikat pro Domäne erworben und verwaltet werden muss. Ein Nachteil kann sein, wenn die Kommunikationspartner die Technik von Mail-Gateway-Zertifikaten (noch) nicht verstehen. Dann wird die Signatur als ungültig angezeigt.

### 4.6.8 Konfiguration des MailSealers

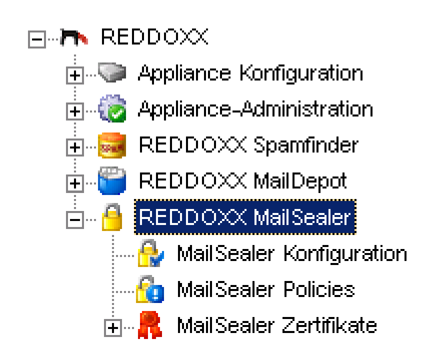



Abbildung: Navigationsbaum REDDOXX MailSealer

### 4.6.8.1 Konfiguration

**Allgemeine Einstellungen**

1. Wählen Sie den Reiter „Allgemeine Einstellungen“ aus.
   Folgender Dialog geht auf:

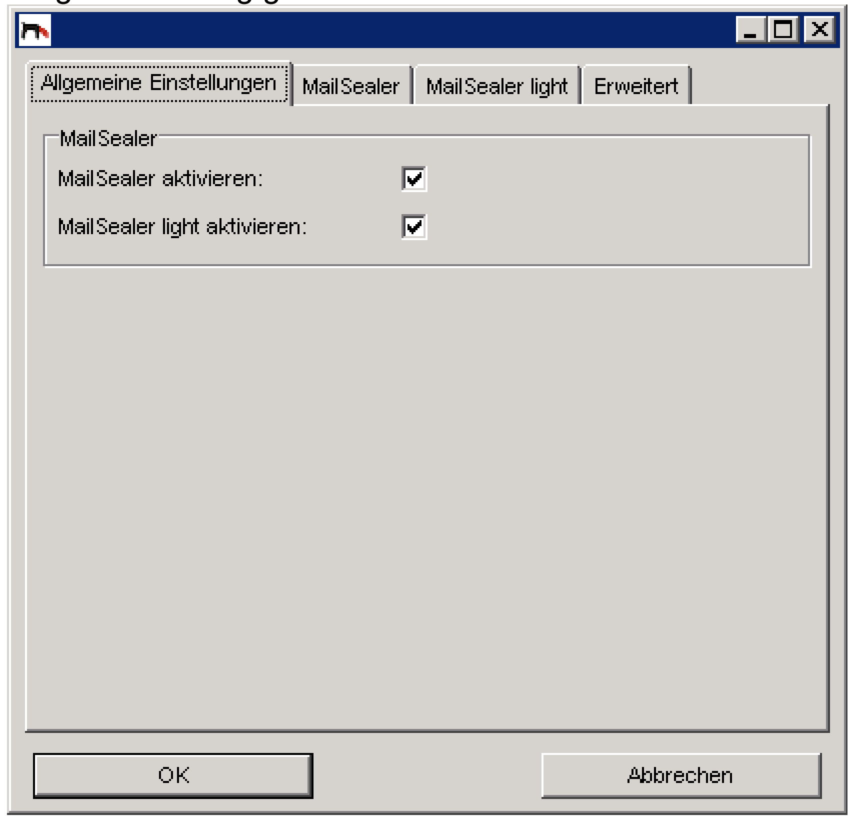



Abbildung: MailSealer - Allgemeine Einstellungen

2. Aktivieren Sie die Checkboxen der Verschlüsselungsverfahren, die Sie nutzen wollen. Falls beide aktiv sind, überprüft zuerst der MailSealer, ob eine entsprechende Policy greift. Falls ja, wird der MailSealer Light **nicht** mehr ausgeführt. Einzige Ausnahme ist dabei, wenn die Policy keine Signierung und keine Verschlüsselung aktiviert hat.
3. Beenden Sie den Dialog mit OK. Alle Änderungen sind sofort gültig.

**MailSealer**

1. Wählen Sie den Reiter „MailSealer“ aus.
   Folgender Dialog geht auf:

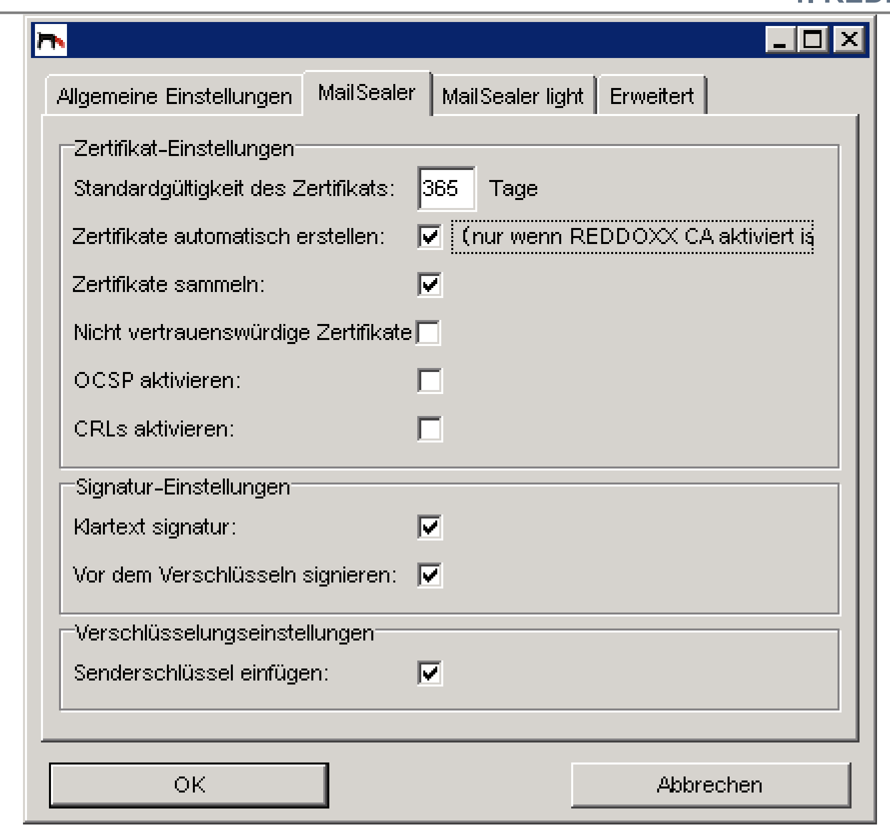


Abbildung: MailSealer – Konfiguration des MailSealers

**Zertifikatseinstellungen:**

2. **Standardgültigkeit des Zertifikats:**
   Gültigkeitsdauer eines automatisch erstellten Zertifikates in Tagen (siehe nachfolgender Punkt). Der Standardwert 365 entspricht genau einem Jahr.
3. **Zertifikate automatisch erstellen:**
   Ist die REDDOXX CA (Certificate Authority) eingerichtet, bekommt jede Absender-E-Mailadresse, die ein Zertifikat erfordert, beim Versand automatisch ein Zertifikat zugewiesen. Als Zertifizierungsstelle (Aussteller) gilt dabei Ihre REDDOXX Appliance. Der Kommunikationspartner (E-Mail-Empfänger) muss dabei Ihrem REDDOXX Root-Zertifikat vertrauen. Dies erreicht er dadurch, dass er Ihr selbst-signiertes (engl.: self signed) REDDOXX-Root-Zertifikat in seinen Zertifikatsspeicher für Autoritäten (certificate authorities) importiert und auf VERTRAUEN (trusted) einstellt. Der Vorteil der selbst ausstellenden Autorität liegt dabei, dass für sämtliche E-Mailadressen keine kommerziellen Zertifikate erworben werden müssen. Sie müssen lediglich dafür sorgen, dass Ihr Kommunikationspartner Ihr Root-Zertifikat importiert. Sie können ihm dies erleichtern, indem Sie über Ihre Unternehmens-Homepage das Root-Zertifikat zum Download anbieten. Durch ein S/MIME-Zertifikat Ihres Webservers können Sie dem Partner gegenüber dabei Ihre Identität beweisen.
4. **Zertifikate sammeln:**
   Die Public Keys aller eingehenden E-Mails werden im Zertifikatsspeicher für Public Keys gesammelt. Dadurch entfällt das manuelle Importieren von Public Keys. Ist ein Public Key eines E-Mail-Partners bereits vorhanden, kann an ihn bereits verschlüsselt versendet werden. (Voraussetzung dabei

ist, dass der Versender über ein eigenes Zertifikat bzw. Schlüsselpaar verfügt).

5. **Nicht vertrauenswürdige Zertifikate sammeln:**
   Bei einer eingehenden E-Mail kann das Zertifikat als ungültig eingestuft werden, sofern der Aussteller des Zertifikates - noch - nicht im Zertifikatsspeicher (certificate authorities) vorhanden ist. Durch das nachträgliche Eintragen dieses Root-Zertifikates werden dadurch alle bisher als ungültig eingestuften Zertifikate gültig.
   Ist dieser Haken jedoch nicht gesetzt, werden erst gar keine ungültigen Public Keys gespeichert.

6. **OCSP aktivieren:**
   Statusabfrage der Zertifikate über das Online Certificate Status Protocol. Bei jeder Benutzung des Zertifikates wird dessen Gültigkeit Online überprüft. Da derzeit nur wenige Aussteller diesen Service verlässlich anbieten, empfehlen wir Stand März 2008 diese Funktion noch nicht zu benutzen, da es dadurch zu spürbaren Zeitverzögerungen kommen würde (Bedingt durch TimeOuts des Serviceanbietes)

7. **CRLs aktivieren:**
   Abfrage über die Gültigkeit von Zertifikaten.
   Zertifikatsaussteller bieten i.d.R. sogenannte **C**ertificate **R**evocation **L**ists an. Damit kann ein Zertifikat vom Aussteller vorzeitig, also vor Ablauf seiner Gültigkeitsdauer, als ungültig markiert werden, z.B. bei Erkennung von Missbrauch. Die REDDOXX Appliance prüft die CRLs einmal pro Tag ab.

**Signatureinstellungen:**

8. **Klartext Signatur**
   Ist der Haken gesetzt, so wird die Signatur als separater MIME-Part der E-Mail hinzugefügt. Dadurch ist die E-Mail von jedem Mail-Client lesbar, auch wenn der Mail-Client kein S/MIME unterstützt. Nachteil dabei ist, dass dazwischenliegende Mail-Gateways die E-Mail verändern können, z.B. durch Zeilenumbrüche oder zusätzliche Textsignaturen. Dadurch wird die Signatur ungültig.

   Ist der Haken nicht gesetzt, wird die gesamte E-Mail zusammen mit der Signatur Base64 kodiert. Nur S/MIME-fähige Mail-Clients können die E-Mail lesen. Vorteil dabei ist, dass die kodierte E-Mail nicht mehr durch dazwischen liegende Gateways verändert werden kann.

**HINWEIS**

Solange Sie nicht sicherstellen können, dass alle Ihrer Kommunikationspartner einen S/MIME-fähigen Mail-Client benutzen, sollten Sie die Klartext-Signierung verwenden.

9. **Vor dem Verschlüsseln signieren**

   Ist der Haken gesetzt, wird vor dem Verschlüsseln signiert. Der **Vorteil** dabei ist, dass die Signaturinformation von dazwischen liegenden Angreifern (Man-in-the-middle-attack) nicht erkannt werden kann.

   Ist der Haken nicht gesetzt, wird nach dem Verschlüsseln signiert. **Vorteil**:

Der Empfänger kann auch ohne Schlüssel anhand der Signatur eindeutig feststellen, von wem die E-Mail kommt und dass Sie unverändert ist. Möglicherweise kann er seinen Private Key nachträglich installieren und die E-Mail somit entschlüsseln.

**Verschlüsselungseinstellungen**

10. **Senderschlüssel einfügen:**
    Normalerweise wird die E-Mail mit dem Public Key des Empfängers verschlüsselt. Beim Versenden wird die E-Mail, sofern aktiviert, im Maildepot gespeichert. Will sich der Versender diese E-Mail später noch einmal zustellen lassen, würde die Appliance ohne diese alternative Verschlüsselung (mit dem Public Key des Versenders) die E-Mail nicht mehr entschlüsseln können.
11. Beenden Sie den Dialog mit OK. Alle Eingaben sind sofort gültig.

**MailSealer Light**

1. Wählen Sie den Reiter „MailSealer Light“ aus.
   Folgender Dialog geht auf:

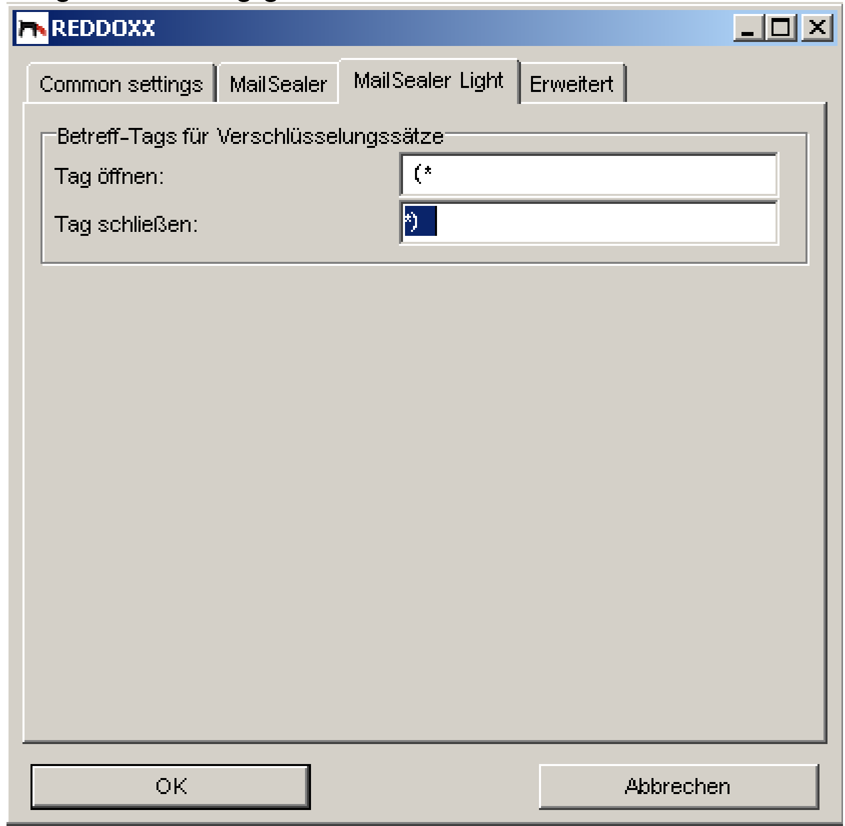



Abbildung: Navigationsbaum REDDOXX MailSealer Light – Konfiguration

**Betreff-Tags für Verschlüsselungssätze**

2. **Tag öffnen**
   Geben Sie hier eine Zeichenfolge ein, mit der Sie den Beginn der Passphrase in der Betreffzeile markieren.
3. **Tag schließen**
   Geben Sie hier eine Zeichenfolge ein, mit der Sie das Ende der Passphrase in der Betreffzeile markieren.
4. Klicken Sie auf OK, um die Konfiguration abzuschließen.
   Alle Eingaben sind sofort gültig.

**Erweitert**

1. Wählen Sie den Reiter „Erweitert" aus.
   Folgender Dialog geht auf:

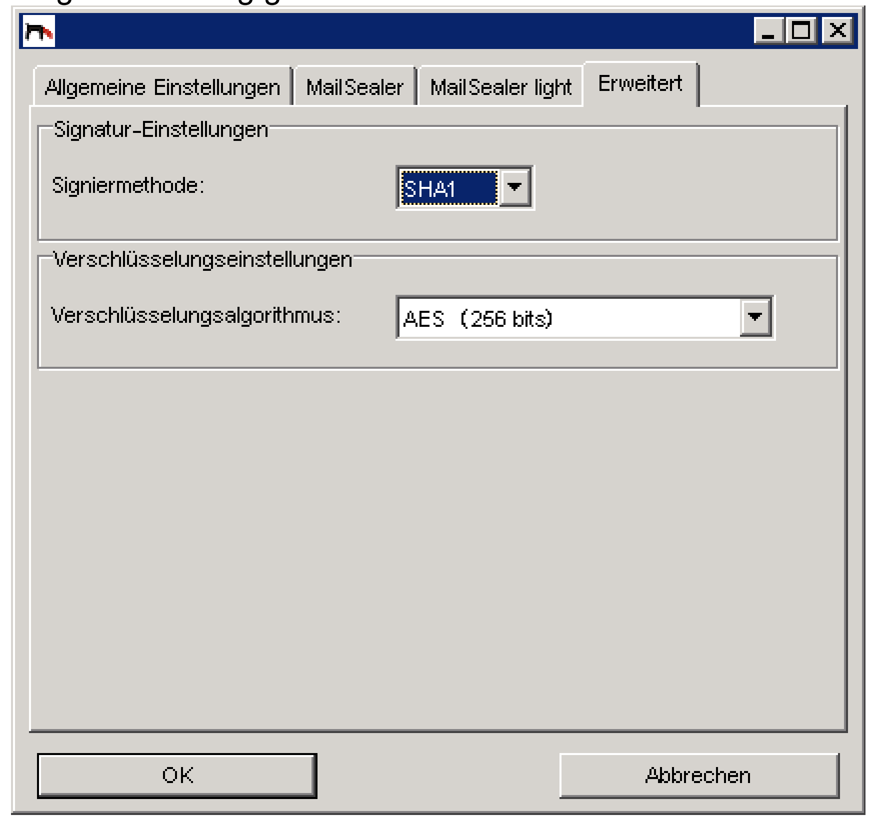



Abbildung: Navigationsbaum REDDOXX MailSealer Light - Konfiguration

2. **Signiermethode:**
   SHA1 (Secure Hash Algorithm)
   MD5 (Message-Digest Algorithm 5)

**Verschlüsselungseinstellungen**

3. **Verschlüsselungsalgorithmus**
   DES (symmetrischer Verschlüsselungsalgorithmus Data Encryption Standard) 3DES (dreifach Data Encryption Standard)
   AES (Advanced Encryption Standard in verschiedenen Schlüssellängen)
4. Klicken Sie auf OK, um die Konfiguration abzuschließen. Alle Eingaben sind sofort gültig.

### 4.6.8.2 Policies

Mit den Policies können Sie definieren wann eine E-Mail verschlüsselt und / oder signiert werden soll.

1. Klicken in der Menüleiste oben auf das Plus-Symbol, um eine neue Policy zu erstellen. Folgender Dialog geht auf:

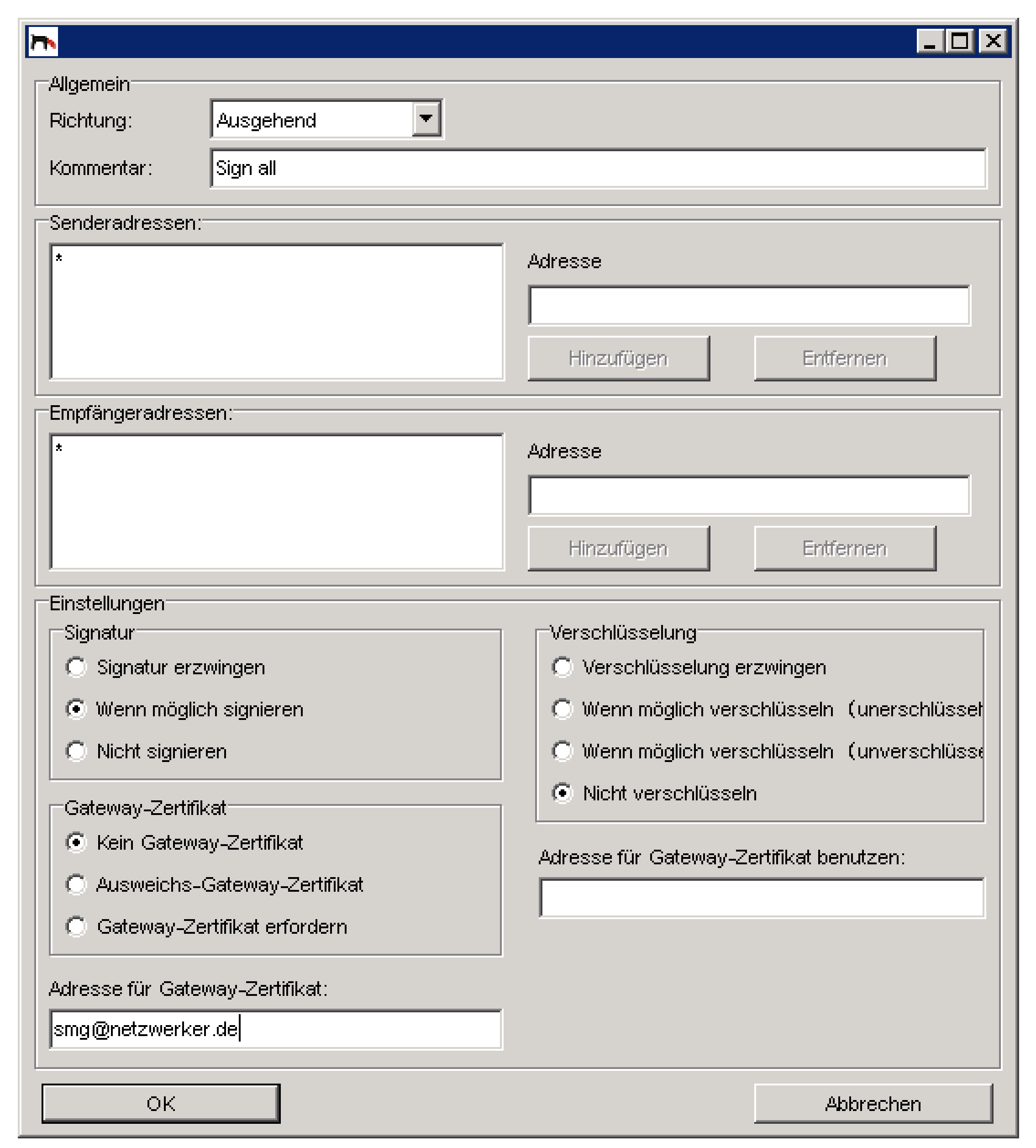



Abbildung: Navigationsbaum REDDOXX MailSealer - Policies – ausgehende Richtung

**Allgemein:**

2. **Richtung:**
   Sie können Regeln für aus- und eingehende E-Mails festlegen oder eine bereits bestehende Regel deaktivieren. Die nachfolgenden Punkte gelten für eine ***ausgehende*** Richtung.
3. **Kommentar:**
   Geben Sie der neuen Policy einen möglichst treffenden Kommentar. Dieser wird in der

Policy-Liste angezeigt und dient zur Unterscheidung anderer Policies. Im Protokoll können Sie nachvollziehen, ob diese Policy zum Einsatz kam.

4. **Senderadressen:**
   Fügen Sie die Senderadressen ein, für die die Policy gelten soll. Ein „*“ steht für alle. Sie können den Stern (*) auch teilsweise benutzen. Beispiel: *@mydomain.com.
5. **Empfängeradressen:**
   Fügen Sie die Empfängeradressen ein, für die die Policy gelten soll. Der Stern (*) gilt wie unter Punkt 4.

**Einstellungen**
**Signatur:**

6. **Signatur erzwingen**
   Die E-Mail muss auf jeden Fall signiert werden. Ist keine Signatur (Public Key) für den Absender vorhanden, wird die E-Mail nicht versendet sondern an den Absender zurückgeworfen (bounced).
7. **Wenn möglich signieren**
   Ist eine Signatur (Public Key) vorhanden, wird die E-Mail signiert versendet. Ansonsten wird sie unsigniert versendet. Der Absender wird dabei nicht informiert.
8. **Nicht signieren**
   Die E-Mail wird unsigniert versendet.

**Gateway-Zertifikat:**

9. **Kein Gateway-Zertifikat**
   Es wird kein Gateway-Zertifikat verwendet.

   **Ausweichs-Zertifikat**
   Ist für den Sender kein eigenes Zertifikat vorhanden, wird das Gateway-Zertifikat verwendet.

   **Gateway-Zertifikat erfordern**
   Es wird ausschließlich das Gateway-Zertifikat verwendet.

10. **Adresse für Gateway-Zertifikat**
   Tragen Sie hier die E-Mailadresse aus dem Gateway-Zertifikat ein.

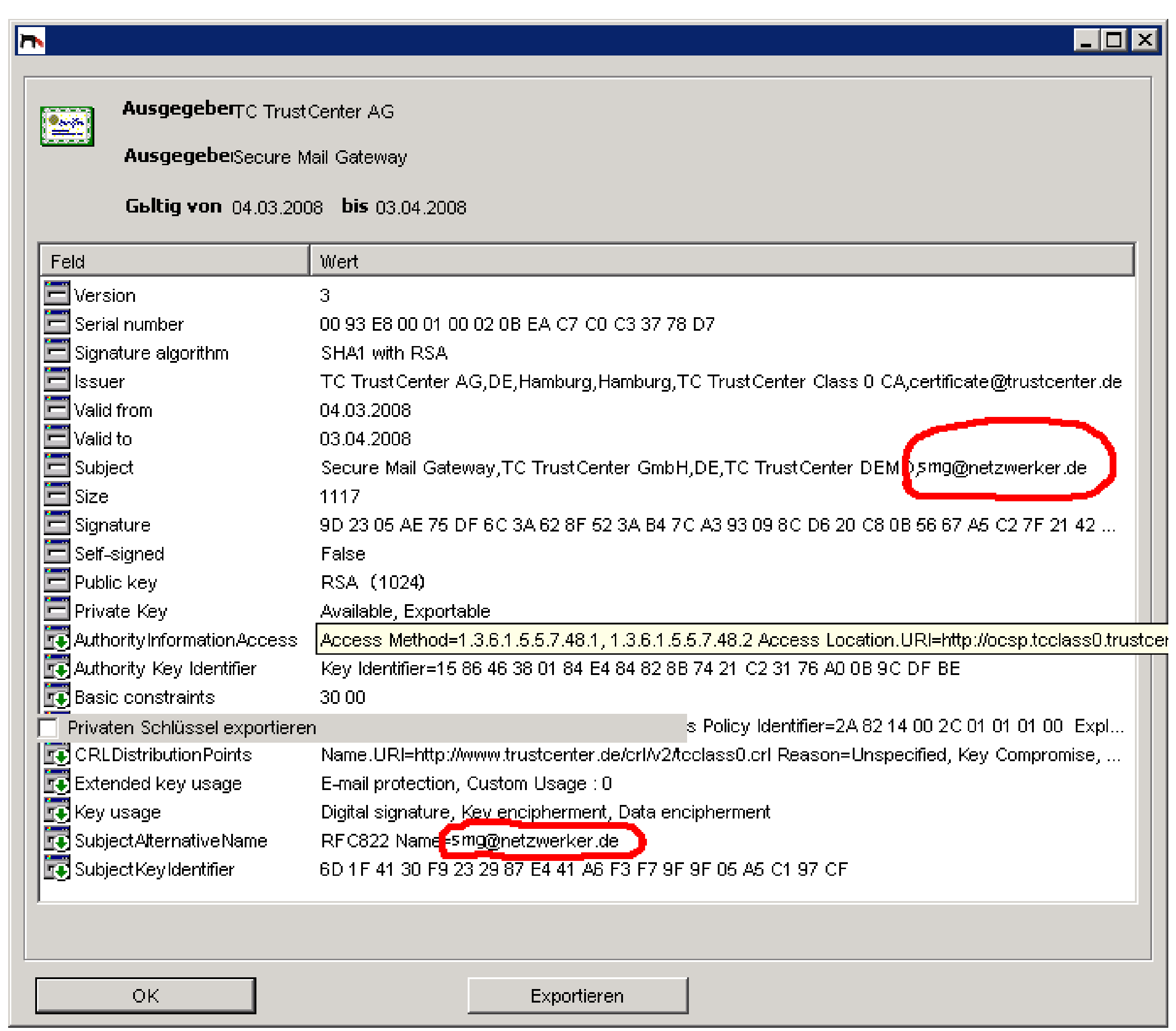


Abbildung: Gateway-Zertifikat

**Encryption – Verschlüsselung:**

11. **Verschlüsselung erzwingen**
    Die E-Mail soll auf jeden Fall verschlüsselt versendet werden. Ist keine Verschlüsselung möglich (z.B.: kein Zertifikat vorhanden), wird die E-Mail nicht versendet, sondern dem Absender zurückgeworfen (bounced).
12. **Wenn möglich verschlüsseln – mit Benachrichtigung**
    Die E-Mail soll verschlüsselt versendet werden. Ist dies nicht möglich wird die E-Mail dennoch unverschlüsselt versendet. Der Absender wird dann darüber informiert (bounce).
13. **Wenn möglich verschlüsseln – ohne Benachrichtigung**
    Sofern möglich, wird die E-Mail verschlüsselt versendet. Falls eine Verschlüsselung nicht möglich ist, wird sie unverschlüsselt versendet. Der Absender wird nicht informiert.
14. **Nicht verschlüsseln**
    Die E-Mail wird auf keinen Fall verschlüsselt versendet.

Die nachfolgenden Punkte gelten für eine ***eingehende*** Richtung.

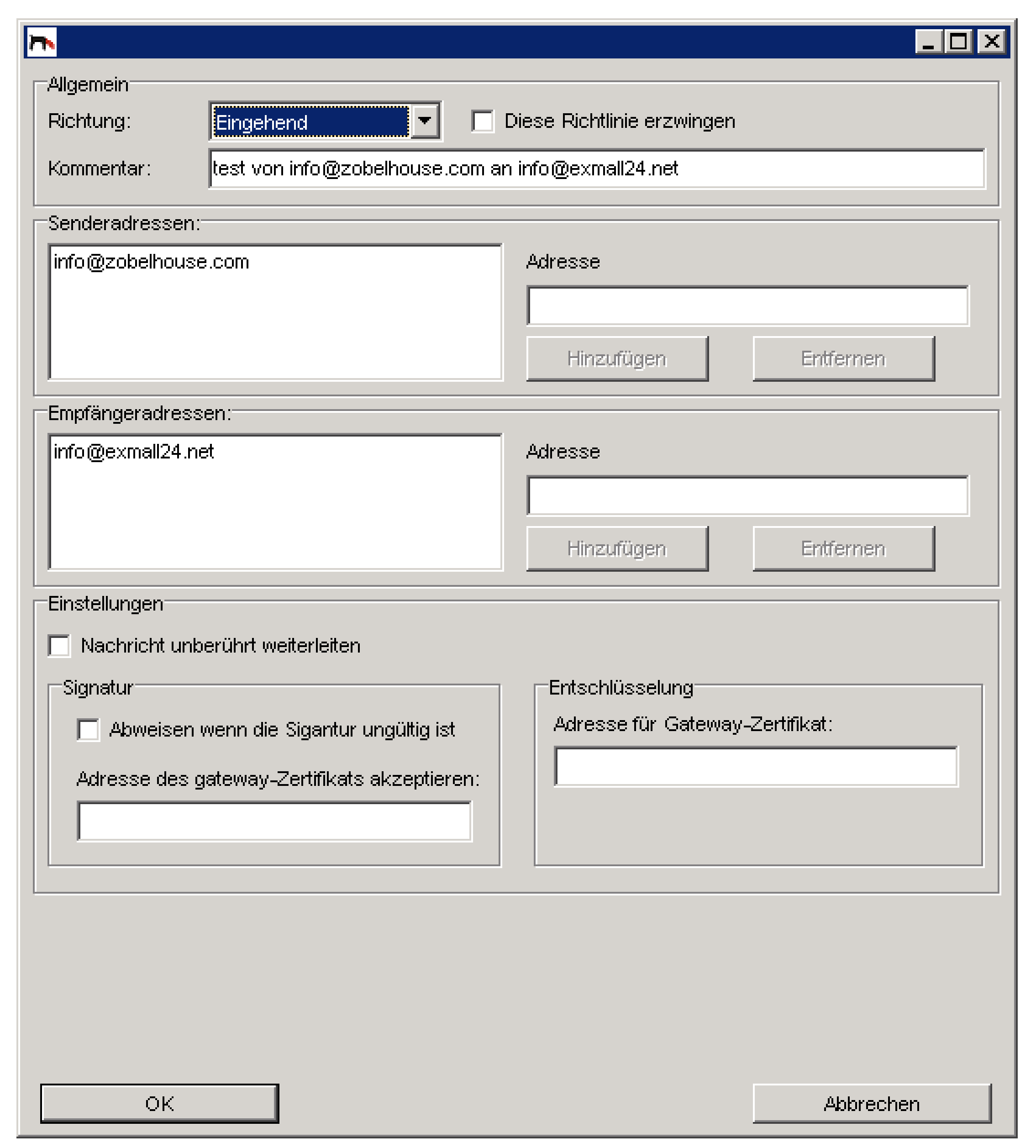



Abbildung: Navigationsbaum REDDOXX MailSealer - Policies – eingehende Richtung

**Allgemein:**

1. **Richtung:**
   Sie können Regeln für aus- und eingehende E-Mails festlegen oder eine bereits bestehende Regel deaktivieren. Die nachfolgenden Punkte gelten für eine ***eingehende*** Richtung.
2. **Diese Richtlinie erzwingen**
   Aktivieren Sie die Checkbox wenn Sie bei mehreren zutreffenden Richtlinien (Policies), das Ausführen dieser Richtlinie erzwingen möchten. Alle anderen Richtlinien werden dann nicht weiter berücksichtigt.
3. **Kommentar:**
   Geben Sie der neuen Policy einen möglichst treffenden Kommentar. Dieser wird in der Policy-Liste angezeigt und dient zur Unterscheidung anderer Policies. Im Protokoll können Sie nachvollziehen, ob diese Policy zum Einsatz kam.

4. **Senderadressen:**
   Fügen Sie die Senderadressen ein, für die die Policy gelten soll. Ein „*“ steht für alle. Sie können den Stern (*) auch teilsweise benutzen. Beispiel: *@mydomain.com.
5. **Empfängeradressen:**
   Fügen Sie die Empfängeradressen ein, für die die Policy gelten soll. Der Stern (*) gilt wie unter Punkt 4.

**Einstellungen**

6. **Nachricht unberührt weiterleiten**
   Beispiel: Die E-Mail soll nicht über das REDDOXX Gateway, sondern beim Client direkt entschlüsselt werden. Die E-Mail wird somit unverändert zugestellt.
7. **Abweisen falls Signatur ungültig ist**
   Wurde die Signatur unterwegs verändert, wird die E-Mail nicht angenommen, sondern dem Absender zurückgeworfen (bounced).

### 4.6.8.3 Zertifikate




Abbildung: Navigationsbaum REDDOXX MailSealer - MailSealer Zertifikate

#### 4.6.8.3.1 Private Zertifikate

Hier können Sie Private Zertifikate hinzufügen, löschen, bearbeiten, exportieren oder den Trust Status (Vertrauensstellung) verändern.

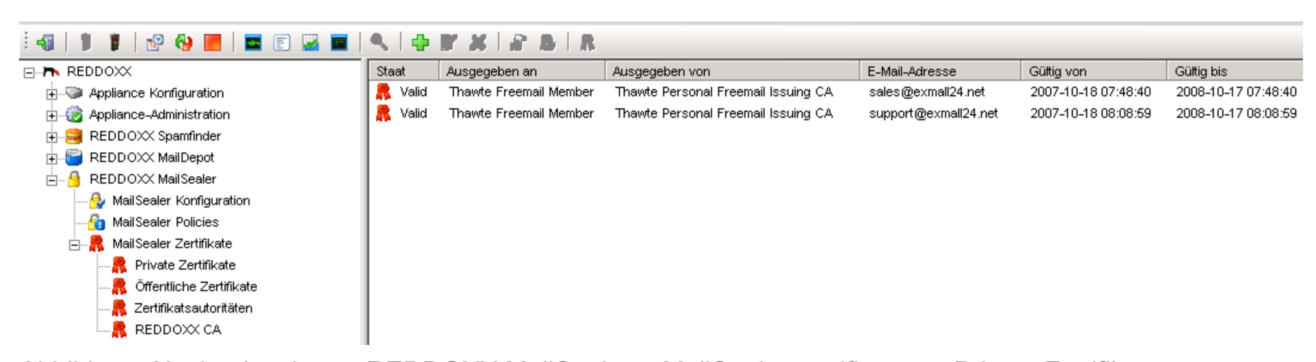
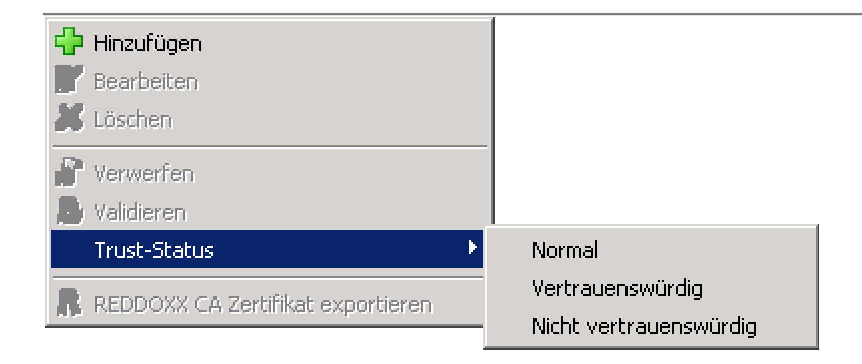



Abbildung: Navigationsbaum REDDOXX MailSealer - MailSealer certificates - Private Zertifikate

Durch Klicken auf ein Zertifikat mit der rechten Maustaste bekommen Sie folgendes Kontext-Menü zu Auswahl angezeigt:




**Private Zertifikate hinzufügen**

1. Klicken Sie in der Menüleiste oben auf das Plus-Symbol oder klicken Sie mit der rechten Maustaste in der Listenansicht, um eine neues privates Zertifikat hinzuzufügen. Folgender Dialog geht auf:

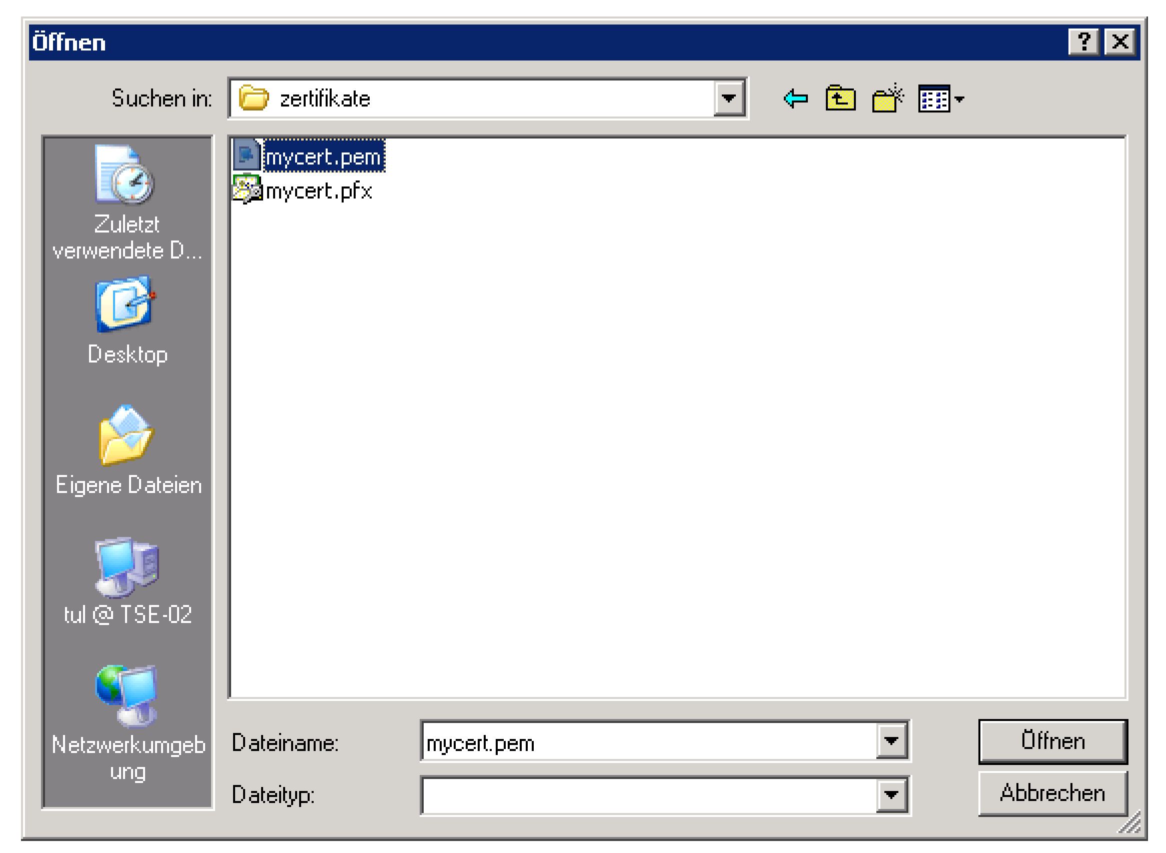



Abbildung: MailSealer - Privates Zertifikat hinzufügen

2. Wählen Sie das hinzuzufügende private Zertifikat aus und klicken Sie auf „*Öffnen*". Nach erfolgreichem Hinzufügen erscheint das Zertifikat in der Liste.

| **HINWEIS** |
|---|
| Derzeit werden nur die beiden Dateiformate PEM und PFX unterstützt. |

3. Geben Sie das Password für den Privaten Schlüssel ein.




Abbildung: Passworteingabe beim Hinzufügen eines privaten Zertifikates.

**Private Zertifikate bearbeiten und exportieren**

1. Mit der Auswahl „Bearbeiten“ im Kontextmenü oder einem Doppelklick auf das private Zertifikat werden Ihnen die Zertifikationsinformationen in einem neuen Dialogfenster angezeigt.

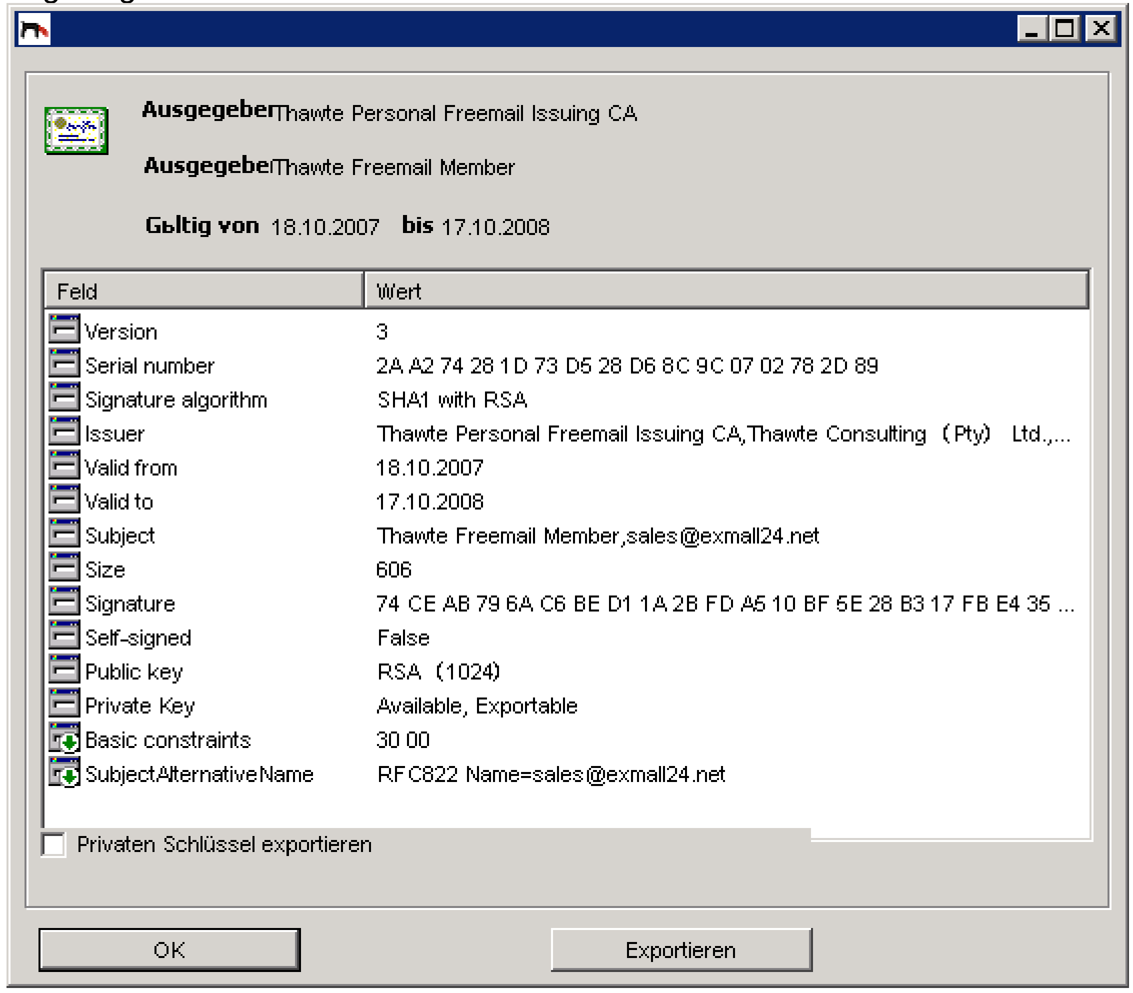



Abbildung: Zertifikationsinformationen

2. **Privaten Schlüssel exportieren:**
   Setzen Sie den Haken, wenn Sie den privaten Schlüssel ebenfalls exportieren wollen. Ist der Haken nicht gesetzt, wird nur der öffentliche Schlüssel exportiert.
3. **Exportieren:**
   Mit Klick auf die Schaltfläche „Exportieren“ öffnet sich der Dialog zum Exportieren des privaten Zertifikates.

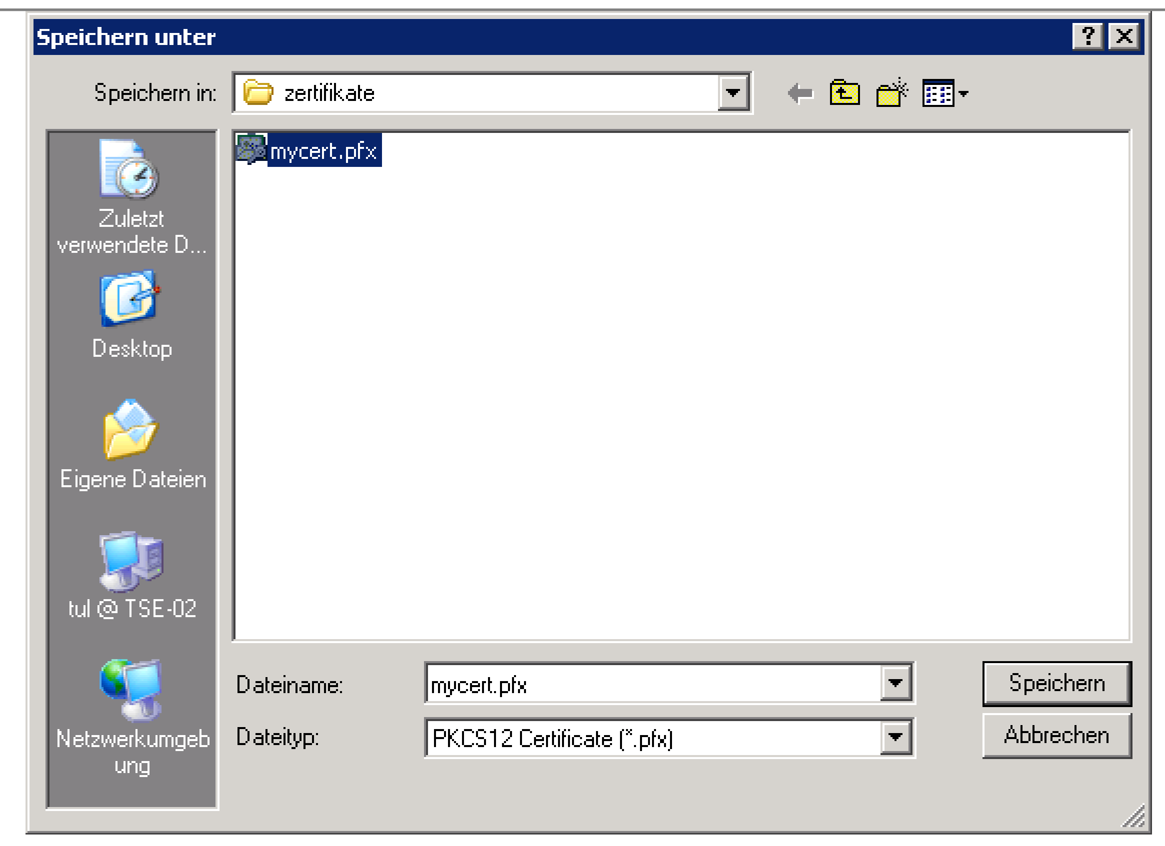



Abbildung: Privates Zertifikat exportieren

4. Wählen Sie einen Dateinamen aus unter dem Sie das Zertifikat exportieren wollen und klicken Sie auf „*Speichern*“.

**HINWEIS**

Wenn Sie auch den privaten Schlüssel exportieren, wählen Sie eines der beiden Dateiformate PEM oder PFX. Das Format CER wird bei privaten Schlüsseln derzeit nicht unterstützt.

5. Geben Sie das Passwort für den privaten Schlüssel ein. Dadurch wird verhindert, dass, wenn jemand in Besitz der Datei kommen sollte, er den privaten Schlüssel importieren kann.

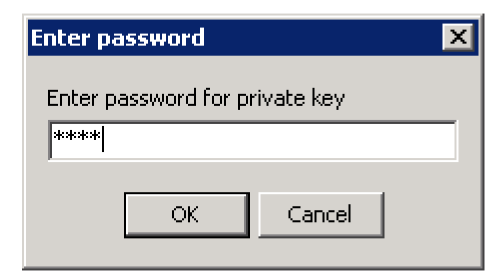



Abbildung: Passworteingabe beim Exportieren eines privaten Zertifikates.

**HINWEIS**

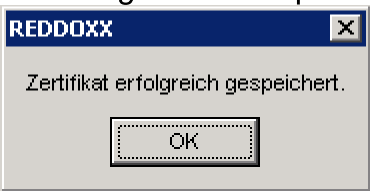
Sie müssen beim Exportieren eines privaten Schlüssels ein Passwort auswählen, da Sie sonst beim Import auf einer anderen REDDOXX Appliance einen Fehler angezeigt bekommen und

der Import abgebrochen wird.




Abbildung: Passworteingabe beim Exportieren eines privaten Zertifikates.

Bei erfolgreichem Exportieren erscheint nachfolgende Bestätigung.




**HINWEIS**

Bereits vorhandene Zertifikats-Dateien werden ungefragt überschrieben!

**Private Zertifikate löschen**

1. Markieren Sie das Zertifikat, das Sie löschen möchten, eine Mehrfachauswahl ist möglich. Mit der Auswahl „Löschen“ im Kontextmenü oder durch Drücken der ENTF-Taste wird nachfolgende Sicherheitsabfrage angezeigt.

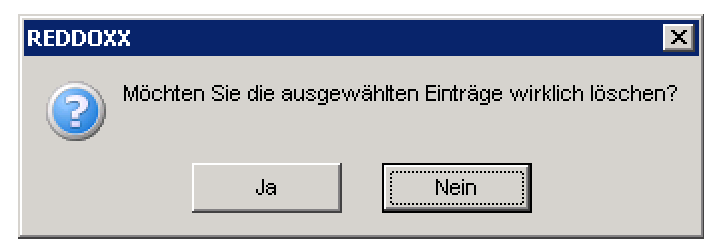



Abbildung: Sicherheitsabfrage beim Löschen eines privaten Zertifikates.

2. Durch Bestätigung mit „Ja“ werden die Zertifikate gelöscht. Die Löschung ist sofort wirksam.

**Private Zertifikate verwerfen**

Diese Funktion ist nur dann aktiv, wenn das Zertifikat über die REDDOXX-eigene CA (Autorisierungsstelle) ausgestellt wurde. Damit können Sie ein bereits ausgestelltes Zertifikat sperren (verwerfen).

1. Klicken Sie rechts auf das Zertifikat und wählen Sie „Verwerfen“.

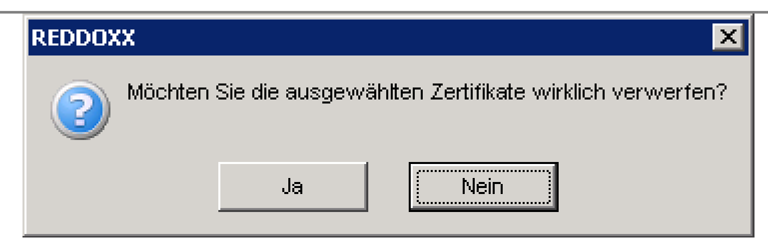



Abbildung: Sicherheitsabfrage beim Verwerfen eines privaten Zertifikates.

2. Durch Bestätigung mit „Ja“ werden die Zertifikate gesperrt. Die Sperrung ist sofort wirksam. Drücken Sie die F5-Taste, um die Anzeige zu aktualisieren. Der Status wird nun als REVOKED angezeigt.

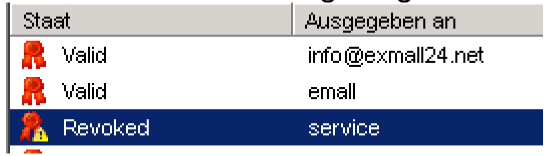



Abbildung: Statusanzeige nach dem Verwerfen (Sperren) eines privaten Zertifikates.

**Private Zertifikate validieren**

Das private Zertifikat wird beim Hinzufügen auf Gültigkeit geprüft. Es wird außerdem jedes Mal geprüft, wenn es bei einem Mailein- oder Ausgang verwendet wird.

Folgende Punkte werden geprüft:

- Gültigkeitszeitraum des privaten Zertifikates (Wird bei der Ausstellung festgelegt.)
- Steht das Zertifikat auf der Revocation List (CRL)?
- Gibt es im Zertifikatsautoritätenspeicher ein gültiges Zertifikat des Ausstellers?

Fehlt das Zertifikat des Ausstellers, so besorgen Sie sich dieses und fügen Sie es dem Zertifikatsautoritätenspeicher hinzu. Danach wählen Sie das private Zertifikat, das Sie erneut überprüfen lassen möchten und klicken auf „Validieren“.

**HINWEIS**

Das Zertifikat eines Ausstellers erhalten Sie üblicherweise auf deren Homepage zum Download. Beispiel: http://www.thawte.com/roots

**Private Zertifikate - Trust Status**

Mögliche Einstellungen sind:

***Normal:*** Das Zertifikat wird auf Gültigkeit/Vertrauenswürdigkeit überprüft.

***Vertrauenswürdig***: Das Zertifikat wird nicht überprüft. Es ist vertrauenswürdig.

***Nicht vertrauenswürdig:*** Das Zertifikat wird nicht überprüft. Es ist nicht vertrauenswürdig.

### 4.6.8.3.2 Öffentliche Zertifikate

Hier können Sie öffentliche Zertifikate hinzufügen, löschen, bearbeiten, exportieren oder den Trust Status (Vertrauensstellung) verändern. Sofern die Funktion zum automatischen Einsammeln von öffentlichen Zertifikaten aktiviert ist (siehe MailSealer-Konfiguration 4.6), sehen Sie hier auch die bereits eingesammelten Zertifikate.

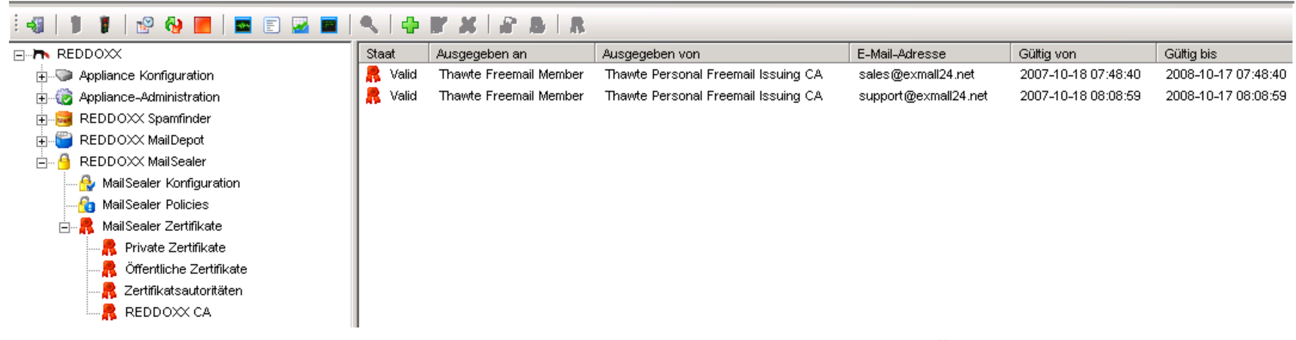
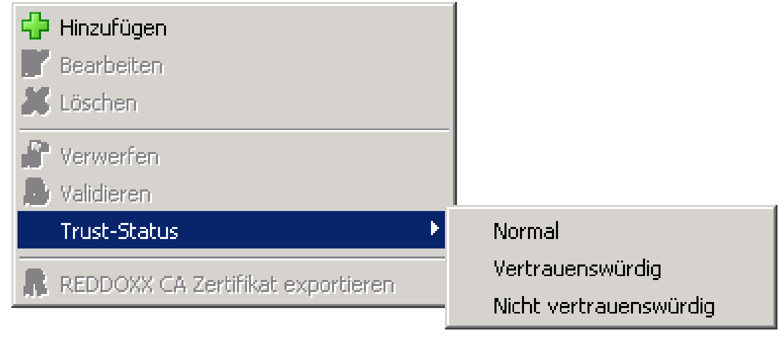



Abbildung: Navigationsbaum REDDOXX MailSealer - MailSealer Zertifikate - Öffentliche Zertifikate

Durch Klicken auf ein Zertifikat mit der rechten Maustaste bekommen Sie folgendes Kontext-Menü zu Auswahl angezeigt:




## Öffentliche Zertifikate hinzufügen

1. Klicken in der Menüleiste oben auf das Plus-Symbol oder klicken Sie mit der rechten Maustaste in die Listenansicht, um eine neues öffentliches Zertifikat hinzuzufügen. Folgender Dialog geht auf:

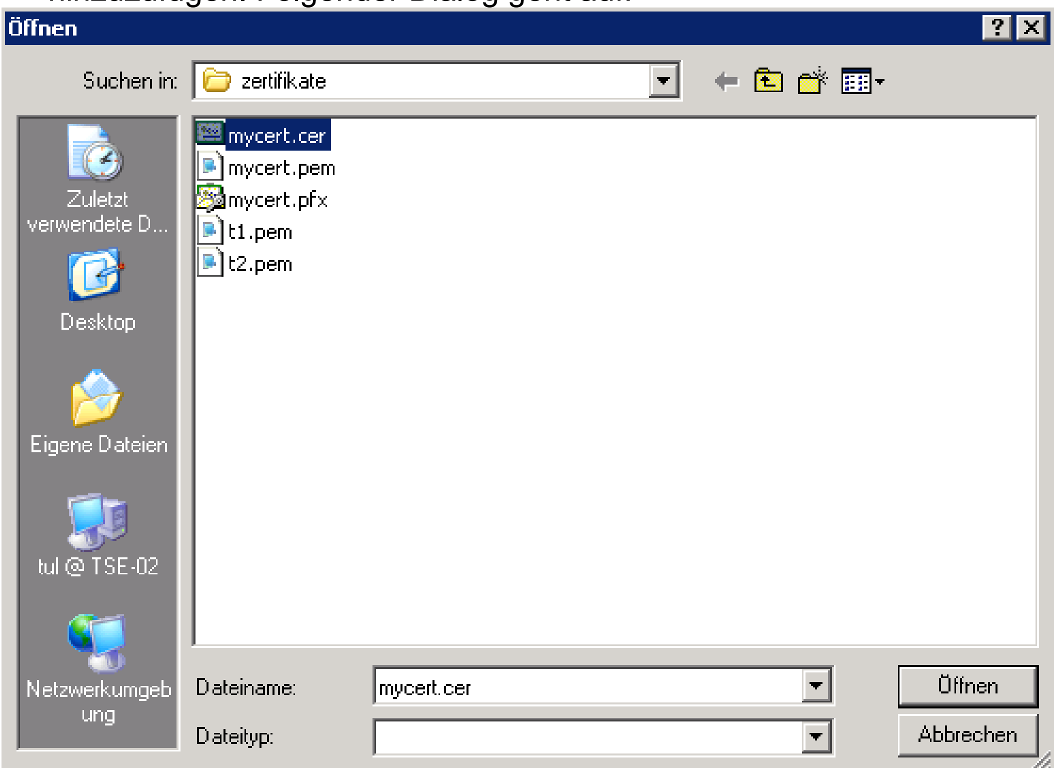



Abbildung: MailSealer - Öffentliches Zertifikat hinzufügen

2. Wählen Sie das hinzuzufügende öffentliche Zertifikat aus und klicken Sie auf „*Öffnen*". Nach erfolgreichem Hinzufügen erscheint das Zertifikat in der Liste.

**Öffentliche Zertifikate bearbeiten und exportieren**

1. Mit der Auswahl „Bearbeiten" im Kontextmenü oder einem Doppelklick auf das öffentliche Zertifikat werden Ihnen die Zertifikats-Informationen in einem neuen Dialogfenster angezeigt.

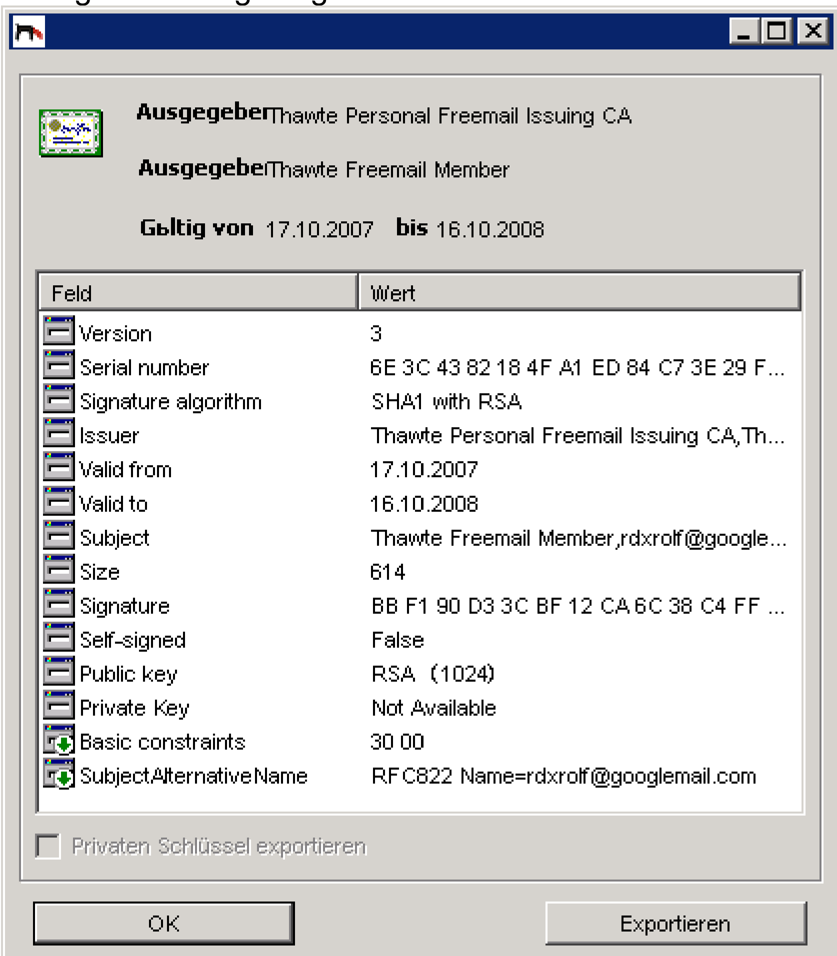



Abbildung: Zertifikationsinformationen

2. **Privaten Schlüssel exportieren:**
   ist bei öffentlichen Schlüsseln nicht möglich und daher deaktiviert.

3. **Exportieren:**
   Mit Klick auf die Schaltfläche „Exportieren" öffnet sich der Dialog zum Exportieren des öffentlichen Zertifikates.

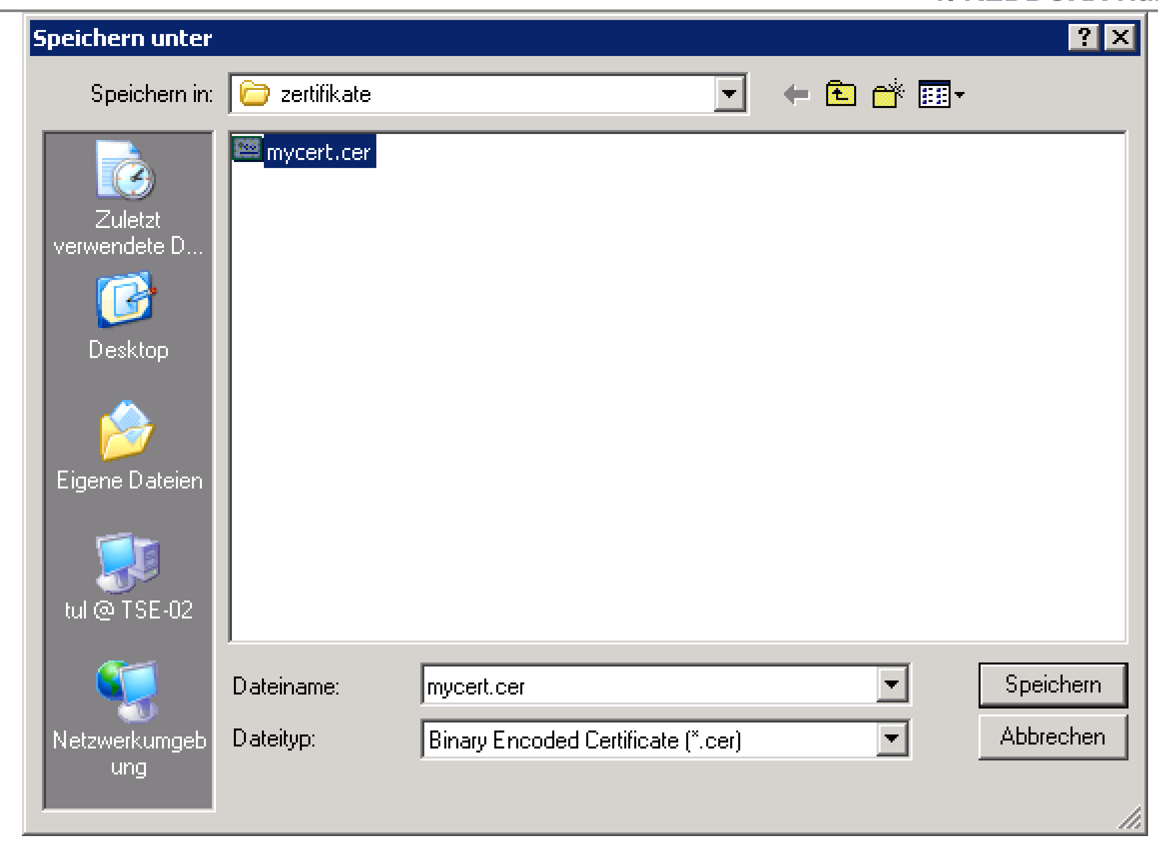



Abbildung: Öffentliches Zertifikat exportieren

4. Wählen Sie einen Dateinamen aus unter dem Sie das Zertifikat exportieren wollen und klicken Sie auf „*Speichern*“.




**HINWEIS**

Bereits vorhandene Zertifikats-Dateien werden ungefragt überschrieben!

## Öffentliche Zertifikate löschen

1. Markieren Sie das Zertifikat, das Sie löschen möchten, eine Mehrfachauswahl ist möglich. Mit der Auswahl „Löschen“ im Kontextmenü oder durch Drücken der ENTF-Taste wird nachfolgende Sicherheitsabfrage angezeigt.

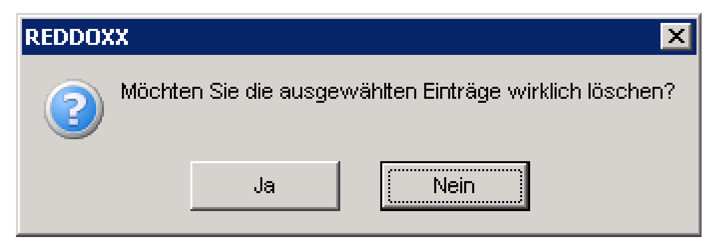



Abbildung: Sicherheitsabfrage beim Löschen eines öffentlichen Zertifikates.

2. Durch Bestätigung mit „Ja“ werden die Zertifikate gelöscht. Die Löschung ist sofort wirksam.

**Öffentliche Zertifikate verwerfen**

Diese Funktion ist nur dann aktiv, wenn das Zertifikat über die REDDOXX-eigene CA (Autorisierungsstelle) ausgestellt wurde. Damit können Sie ein bereits ausgestelltes Zertifikat sperren (verwerfen).

1. Klicken Sie rechts auf das Zertifikat und wählen Sie „Verwerfen“.

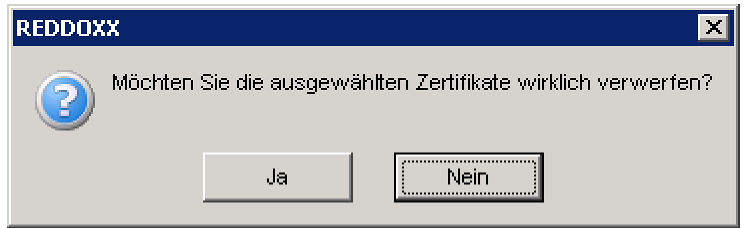



Abbildung: Sicherheitsabfrage beim Verwerfen eines öffentlichen Zertifikates.

2. Durch Bestätigung mit „Ja“ werden die Zertifikate gesperrt. Die Sperrung ist sofort wirksam. Drücken Sie die F5-Taste, um die Anzeige zu aktualisieren. Der Status wird nun als REVOKED angezeigt.

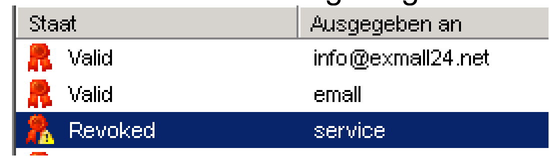



Abbildung: Statusanzeige nach dem Verwerfen (Sperren) eines öffentlichen Zertifikates.

**Öffentliche Zertifikate validieren**

Das öffentliche Zertifikat wird beim Hinzufügen auf Gültigkeit geprüft. Es wird außerdem jedes Mal geprüft, wenn es bei einem Mailein- oder Ausgang verwendet wird.
Folgende Punkte werden geprüft:

- Gültigkeitszeitraum des öffentlichen Zertifikates (Wird bei der Ausstellung festgelegt.)
- Steht das Zertifikat auf der Revocation List (CRL) des Ausstellers?
- Gibt es im Zertifikatsautoritätenspeicher ein gültiges Zertifikat des Ausstellers?

Fehlt das Zertifikat des Ausstellers, so besorgen Sie sich dieses und fügen Sie es dem Zertifikatsautoritätenspeicher hinzu. Danach wählen Sie das öffentliche Zertifikat, das Sie erneut überprüfen lassen möchten und klicken auf „Validieren“.

**HINWEIS**

Das Zertifikat eines Ausstellers erhalten Sie üblicherweise auf deren Homepage zum Download.
Beispiel: http://www.thawte.com/roots

**Öffentliche Zertifikate - Trust Status**

Mögliche Einstellungen sind:
***Normal:*** Das Zertifikat wird auf Gültigkeit/Vertrauenswürdigkeit überprüft.
***Vertrauenswürdig***: Das Zertifikat wird nicht überprüft. Es ist vertrauenswürdig.

***Nicht vertrauenswürdig:*** Das Zertifikat wird nicht überprüft. Es ist nicht vertrauenswürdig.

#### 4.6.8.3.3 Zertifikatsautoritäten

Zertifizierungsautoritäten, auch Aussteller genannt, erstellen Zertifikate. Es gibt kommerzielle und kostenfreie Aussteller. Damit Zertifizierungsautoritäten Zertifikate ausstellen dürfen, benötigen diese ein sogenanntes Root-Zertifikat.  Zertifikate verweisen immer auf einen Aussteller. Beim Prüfen auf Gültigkeit eines Zertifikates werden sämtliche Aussteller in der Ausstellungs-Kette nach oben überprüft. Die Reddoxx hat die gängigsten Zertifizierungsautoritäten bereits eingebaut. Sie müssen jedoch selbst den Vertrauens-Status des Root-Zertifikates auf „*Normal*“ stellen, sofern Sie diesem Aussteller vertrauen.

**HINWEIS**

Die bereits eingebauten Root-Zertifikate sind standardmäßig auf „nicht vertrauenswürdig“ gestellt. Ändern Sie den Status auf „Normal“, wenn Sie einem Aussteller vertrauen. Eine Mehrfachauswahl ist möglich.

**Zertifikatsautoritäten hinzufügen**

1. Klicken in der Menüleiste oben auf  das Plus-Symbol  oder klicken Sie mit der rechten Maustaste in der Listenansicht, um eine neues Root-Zertifikat  hinzuzufügen. Folgender Dialog geht auf:

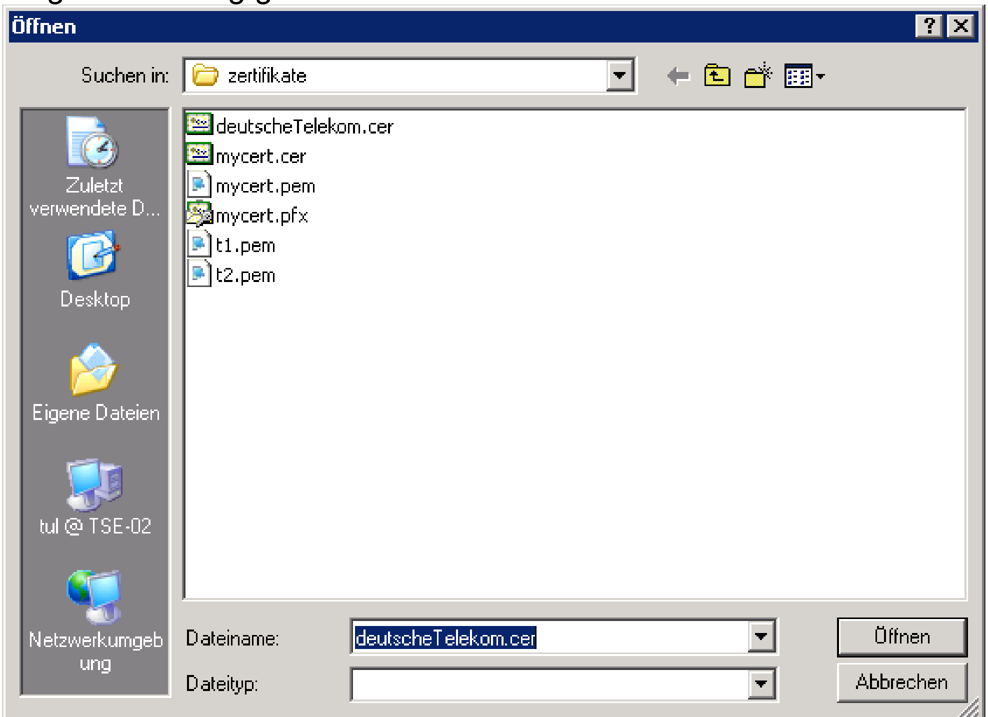



Abbildung: Hinzufügen eines Root-Zertifikates (Zertifikatsautorität)

2. Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf Öffnen. Das Zertifikat wird nun hinzugefügt und in der Liste angezeigt.

**Zertifikatsautoritäten bearbeiten und exportieren**

1. Mit der Auswahl „Bearbeiten“ im Kontextmenü oder einem Doppelklick auf das Root-Zertifikat werden Ihnen die Zertifikationsinformationen in einem neuen Dialogfenster angezeigt.

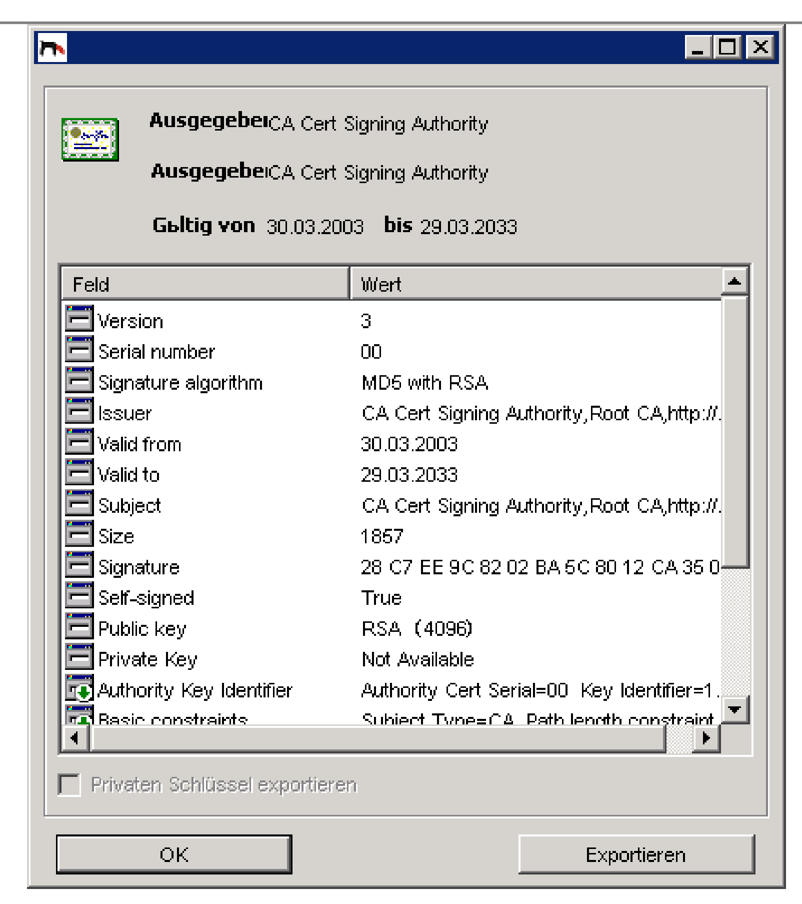



Abbildung: Zertifikationsinformationen

2. Privaten Schlüssel exportieren:
   ist bei hier nicht möglich und daher deaktiviert.
3. Exportieren:
   Mit Klick auf die Schaltfläche „Exportieren“ öffnet sich der Dialog zum Exportieren des Root-Zertifikates.

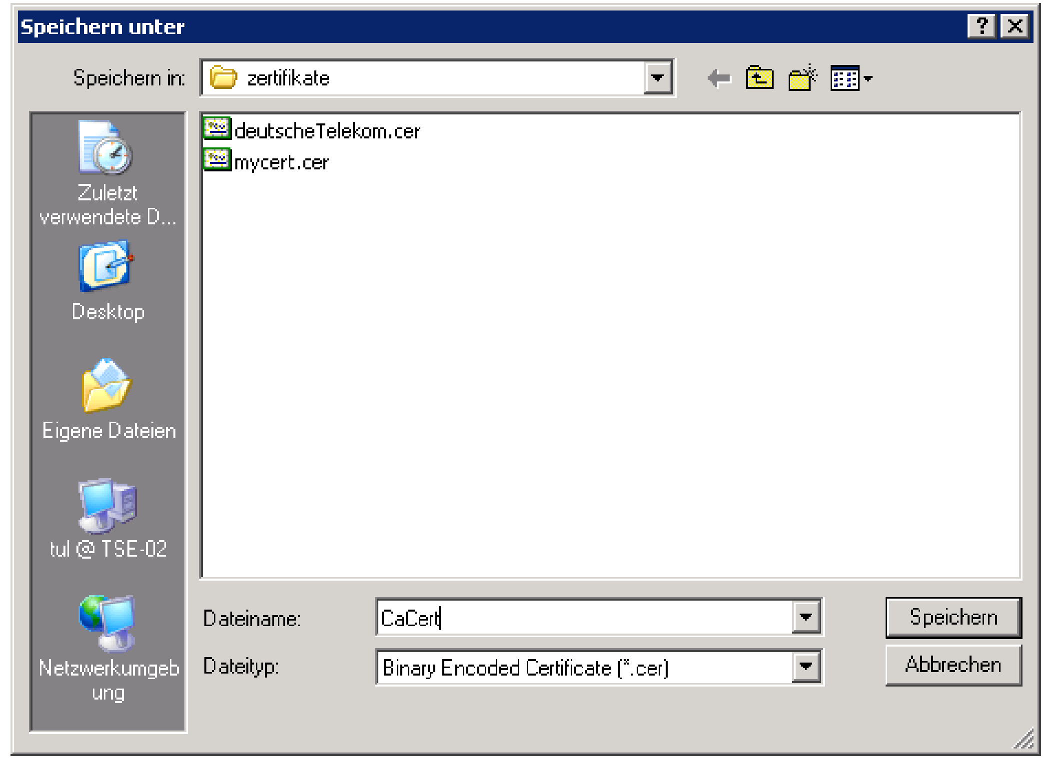


Abbildung: Root-Zertifikat exportieren

4. Wählen Sie einen Dateinamen aus unter dem Sie das Zertifikat exportieren wollen und klicken Sie auf „*Speichern*“.




**HINWEIS**

Bereits vorhandene Zertifikats-Dateien werden ungefragt überschrieben!

### Root-Zertifikate löschen

1. Markieren Sie das Zertifikat, das Sie löschen möchten, eine Mehrfachauswahl ist möglich. Mit der Auswahl „Löschen“ im Kontextmenü oder durch Drücken der ENTF-Taste wird nachfolgende Sicherheitsabfrage angezeigt.

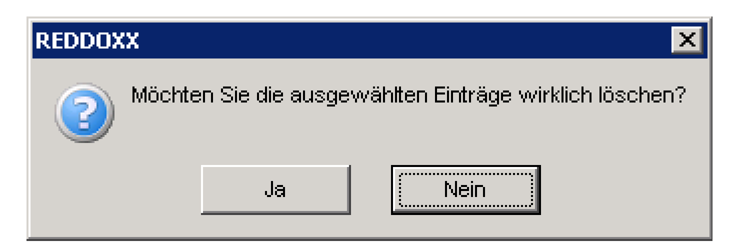



Abbildung: Sicherheitsabfrage beim Löschen eines Root-Zertifikates.

2. Durch Bestätigung mit „Ja“ werden die Zertifikate gelöscht. Die Löschung ist sofort wirksam.

### Root-Zertifikate verwerfen

Diese Funktion ist nur dann aktiv, wenn das Zertifikat über die REDDOXX-eigene CA (Autorisierungsstelle) ausgestellt wurde. Damit können Sie ein bereits ausgestelltes Zertifikat sperren (verwerfen).

3. Klicken Sie rechts auf das Zertifikat und wählen Sie „Verwerfen“.

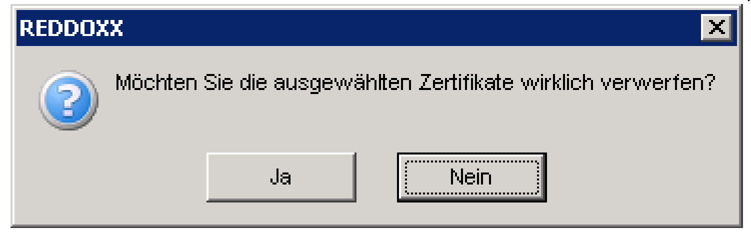



Abbildung: Sicherheitsabfrage beim Verwerfen eines Root-Zertifikates.

4. Durch Bestätigung mit „Ja“ werden die Zertifikate gesperrt. Die Sperrung ist sofort wirksam. Drücken Sie die F5-Taste, um die Anzeige zu aktualisieren. Der Status wird nun als REVOKED angezeigt.

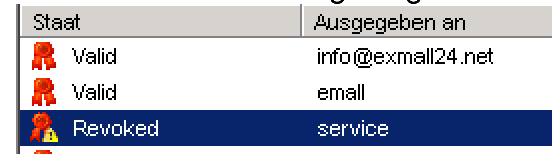


Abbildung: Statusanzeige nach dem Verwerfen (Sperren) eines Root-Zertifikates.

**Root-Zertifikate validieren**
Das Root-Zertifikat wird beim Hinzufügen auf Gültigkeit geprüft. Es wird außerdem jedes Mal geprüft, wenn es bei einem Mailein- oder Ausgang zum Überprüfen der Zertifikate, die von dieser Zertifizierungsautorität ausgestellt wurden, verwendet wird.
Folgende Punkte werden geprüft:

- Gültigkeitszeitraum des Root-Zertifikates (Wird bei der Ausstellung festgelegt.)

**HINWEIS**

Das Root-Zertifikat eines Ausstellers erhalten Sie üblicherweise auf deren Homepage zum Download. Beispiel: http://www.thawte.com/roots

**Root-Zertifikate - Trust Status**
Mögliche Einstellungen sind:
***Normal:*** Das Zertifikat wird auf Gültigkeit/Vertrauenswürdigkeit überprüft.
***Vertrauenswürdig***: Das Zertifikat wird nicht überprüft. Es ist vertrauenswürdig.
***Nicht vertrauenswürdig:*** Das Zertifikat wird nicht überprüft. Es ist nicht vertrauenswürdig.

### 4.6.8.3.4 REDDOXX CA

Mit der REDDOXX eigenen Zertifikationsautorität (CA) können Sie für Ihre E-Mail-Aliase Zertifikate selbst ausstellen bzw. bei Bedarf automatisch durch die Appliance erstellen lassen.
Der Vorteil dabei ist, dass Sie Kosten für den Erwerb von Zertifikaten sowie für die Administration sparen.
Der Nachteil dabei ist, dass die Mail-Empfangsgegenstelle (Empfänger), Ihr Root-Zertifikat einmalig importiert haben muss, damit Ihre Zertifikate als gültig erkannt werden können.

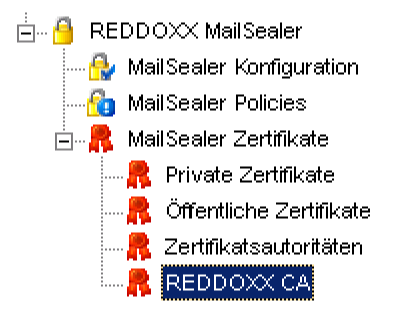



Abbildung: MailSealer – REDDOXX CA – Navigationsbaum

**TIPP**

Um den Austausch Ihres Root-Zertifikates für Ihren Kommunikationspartner zu erleichtern, können Sie Ihr Root-Zertifikat auf einem Ihrer Web-Server zum Download bereitstellen. Vorzugsweise Ist Ihr Web-Server dabei mit einem SSL-Zertifikat ausgestattet, sodass Ihr Kommunikationspartner durch dieses SSL-Zertifikat dem Root-Zertifikat vertrauen kann, das er dort herunterladen kann.

**REDDOXX Root-Zertifikat erstellen**

1. Beim Klick auf „REDDOXX CA“ im Navigationsbaum des MailSealers prüft die Appliance, ob bereits ein Root-Zertifikat vorhanden ist. Das Root-Zertifikat liegt unter Zertifikatsautoritäten. Verwechseln Sie dies also nicht mit der REDDOXX-CA Liste. Dort liegen die personenbezogenen Zertifikate, die mit dem Root-Zertifikat ausgestellt wurden.
2. Falls noch kein Root-Zertifikat vorhanden ist, erscheint nachfolgender Dialog: Klicken Sie auf „JA“ um mit dem Zertifikats-Wizard fortzufahren.

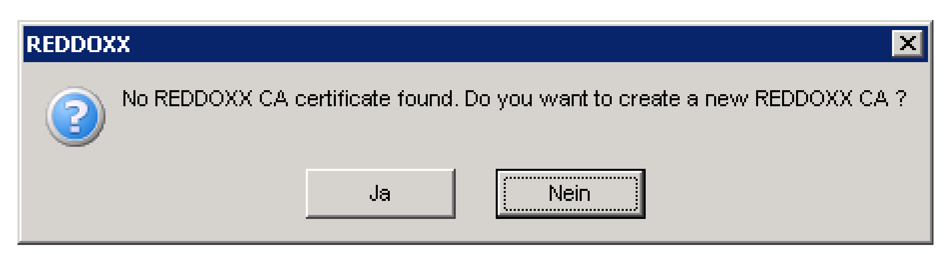



Abbildung: MailSealer – REDDOXX CA – Root-Zertifikat Erstellungsdialog

Es erscheint der Dialog für die Auswahl eines REDDOXX-eigenen Root (CA)-Zertifikates.
Sie haben die Auswahl zwischen einem selbst-signierten Zertifikat und einem erworbenen Zertifikat, das Sie an dieser Stelle hochladen können.

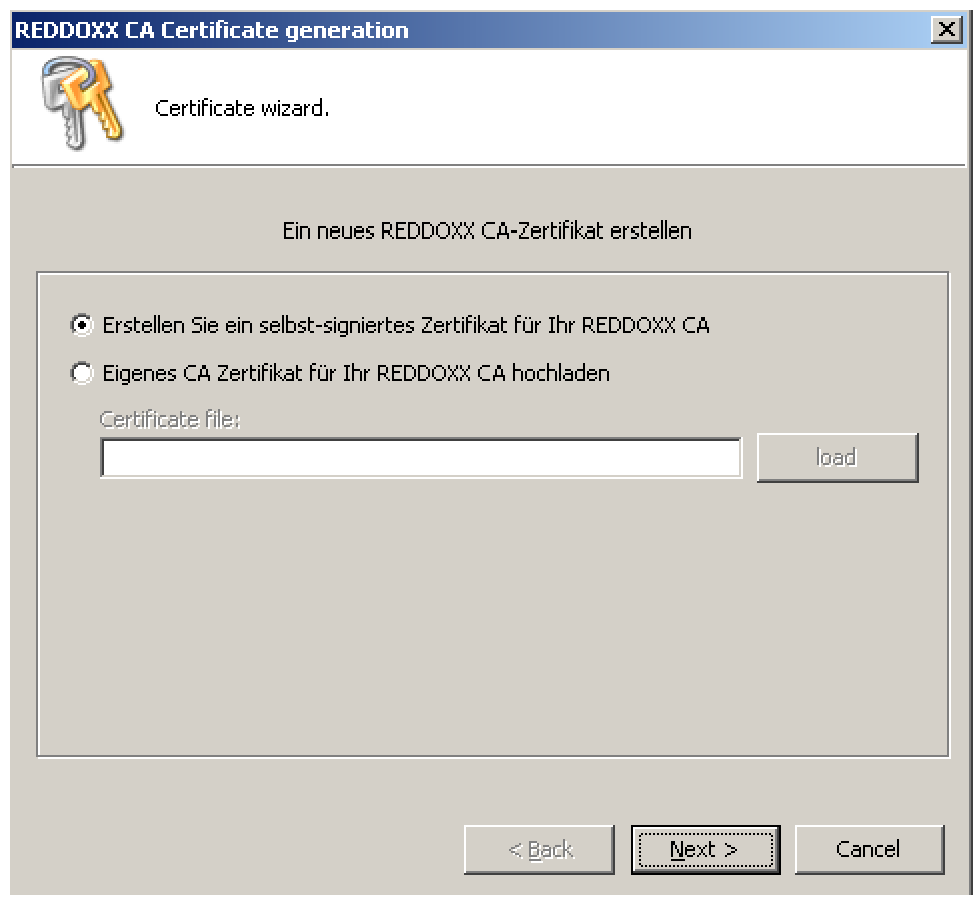



Abbildung: MailSealer – REDDOXX CA – Root Zertifikat Erstellungsdialog

### Selbst-signiertes Root (CA) Zertifikat erstellen

3. Wählen Sie „*Erstellen Sie ein selbst-signiertes Zertifikat für Ihr REDDOXX CA*“ und klicken Sie auf „Next“. Es erscheint folgender Dialog.

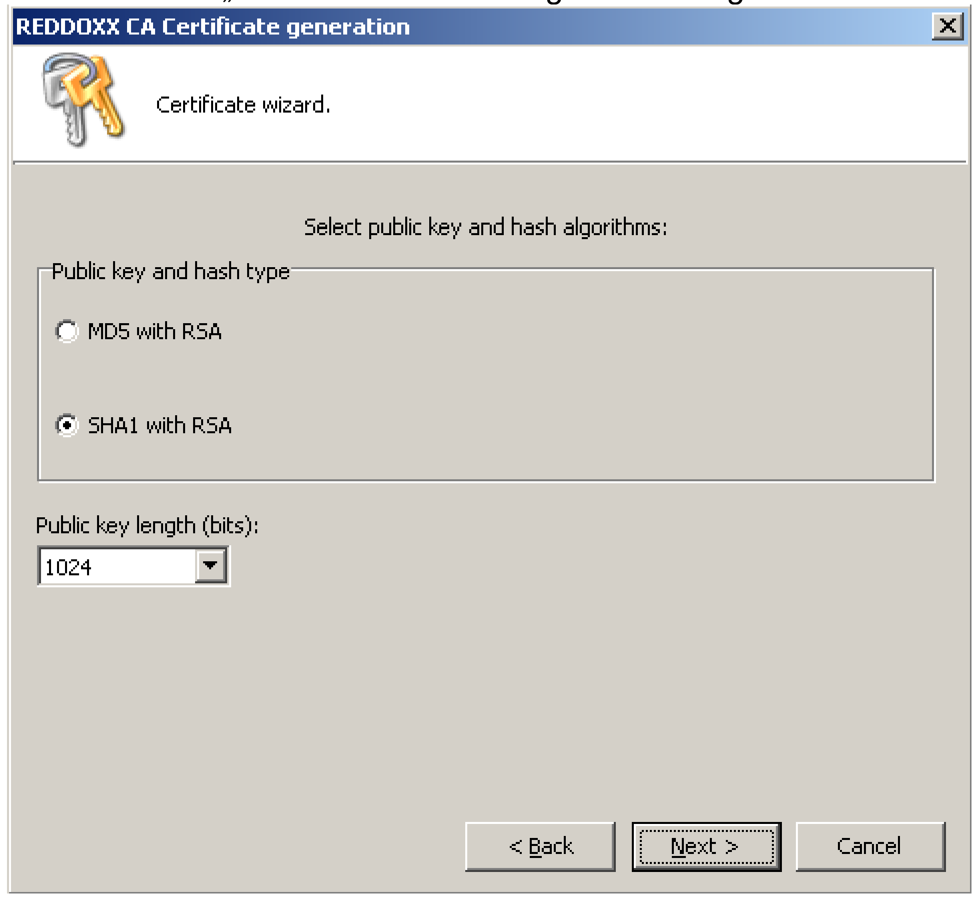



Abbildung: MailSealer – REDDOXX CA – Wizard für das Root-Zertifikat – Schritt 1

Select public key algorithm and hash type:

MD5 with RSA : **M**essage-**D**igest Algorithm **5** als Hash-Funktion und Schlüsselaustausch mit RSA nach **R**ivest, **S**hamir und **A**dleman.

SHA1 with RSA: **S**ecure **H**ash **A**lgorithm und RSA aus Schlüsselaustauschverfahren.

Die Standardvorgabe ist: SHA1 with RSA

4. Public key length (bits) : - Bitlänge des öffentlichen Schlüssels
   Der Standard ist 1024. Wählen Sie zw. 1024 und 2048 Bit.

**HINWEIS**

Je länger der Schlüssel, desto rechenintensiver (Performance) ist die kryptografische Verarbeitung (Signierung und Verschlüsselung). Je länger der Schlüssel, desto höher ist die Sicherheit.

5. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen.

**Subject Parameters: - Eigenschaften des Zertifikates.**
Die Felder sind nur von beschreibender Form und haben keine weitere Funktionalität. Sie dienen zur Information und zur Überzeugung, ob dem Besitzer dieses Zertifikates vertraut werden kann.

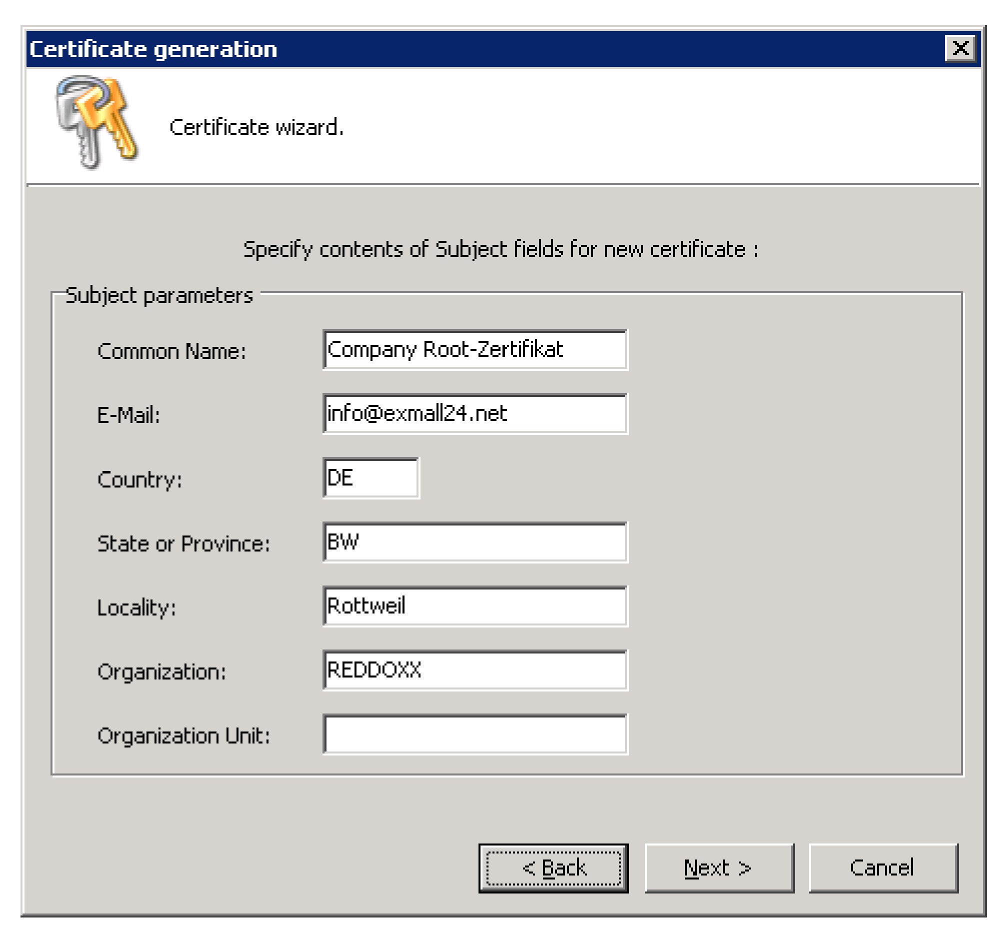



Abbildung: MailSealer – REDDOXX CA – Wizard für das Root-Zertifikat – Schritt 2

1. Common Name : Name / Bezeichnung des Zertifikates
2. E-Mail : Allgemeine E-Mail Adresse des Unternehmens
3. Country : 2 Zeichen Länder-Code (DE, US, GB, FR, ES, CH, AT etc.)
4. State or province : Staat, Bundesland oder Kanton. Beispiele: BW, Baden Württemberg, California, Uri
5. Locality : Stadt, Lokalität
6. Organization : Organisation, Einheit, Tochtergesellschaft
7. Organization Unit : Fachabteilung, Department.

8. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen, auf „BACK“ (Zurück) um zur vorhergehenden Eingabemaske zu gelangen.

**Validity period - Gültigkeitszeitraum**

Die Felder „from“ (von) und „to“ (bis) geben den Gültigkeitszeitraum des Root-Zertifikates an. Dieser Zeitraum wird bei einer E-Mail-Verarbeitung mit überprüft, in der ein durch dieses Root-Zertifikat ausgestelltes persönliches Zertifikat verwendet wird.

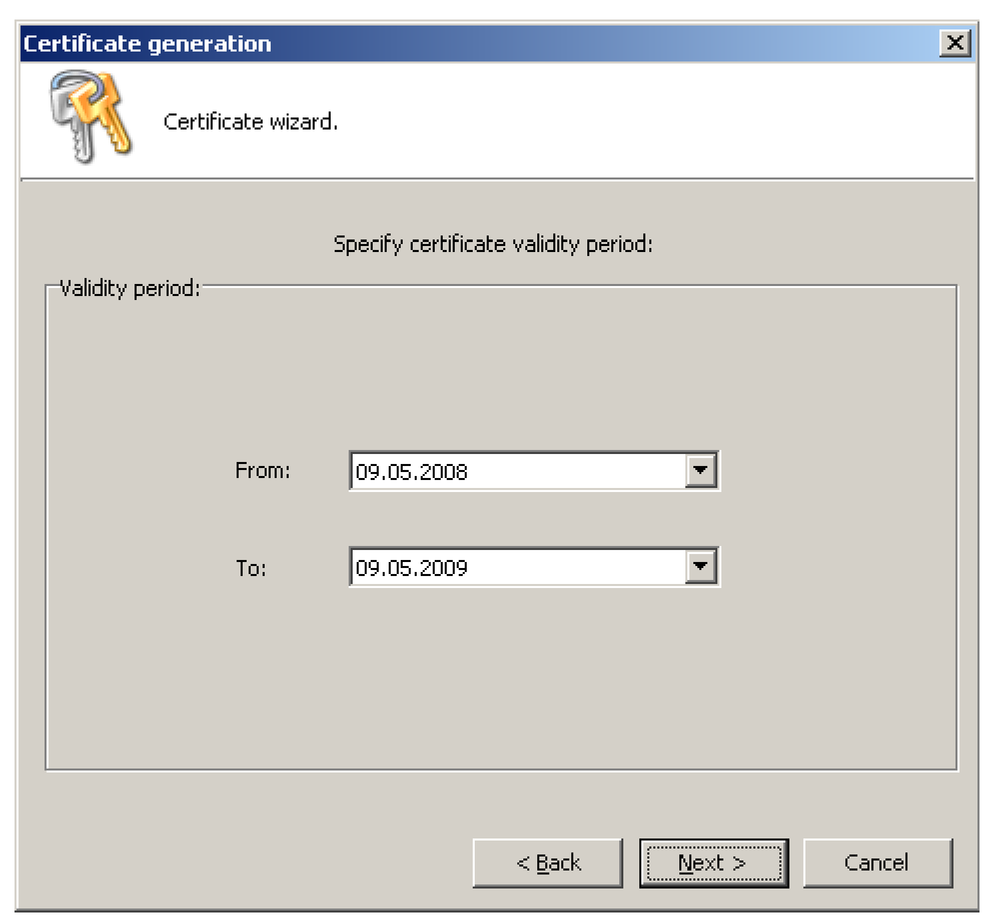



Abbildung: MailSealer – REDDOXX CA – Wizard für das Root-Zertifikat – Schritt 3

1. From (von) : Beginn des Gültigkeitszeitraumes
2. To (bis) : Ende des Gültigkeitszeitraumes
3. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen, auf „BACK“ (Zurück) um zur vorhergehenden Eingabemaske zu gelangen.
4. Zertifikats-Erstellung. Mit Klick auf „GENERATE“ wird das Zertifikat erstellt. Dies dauert einen kleinen Moment (i.d.R. wenige Sekunden).

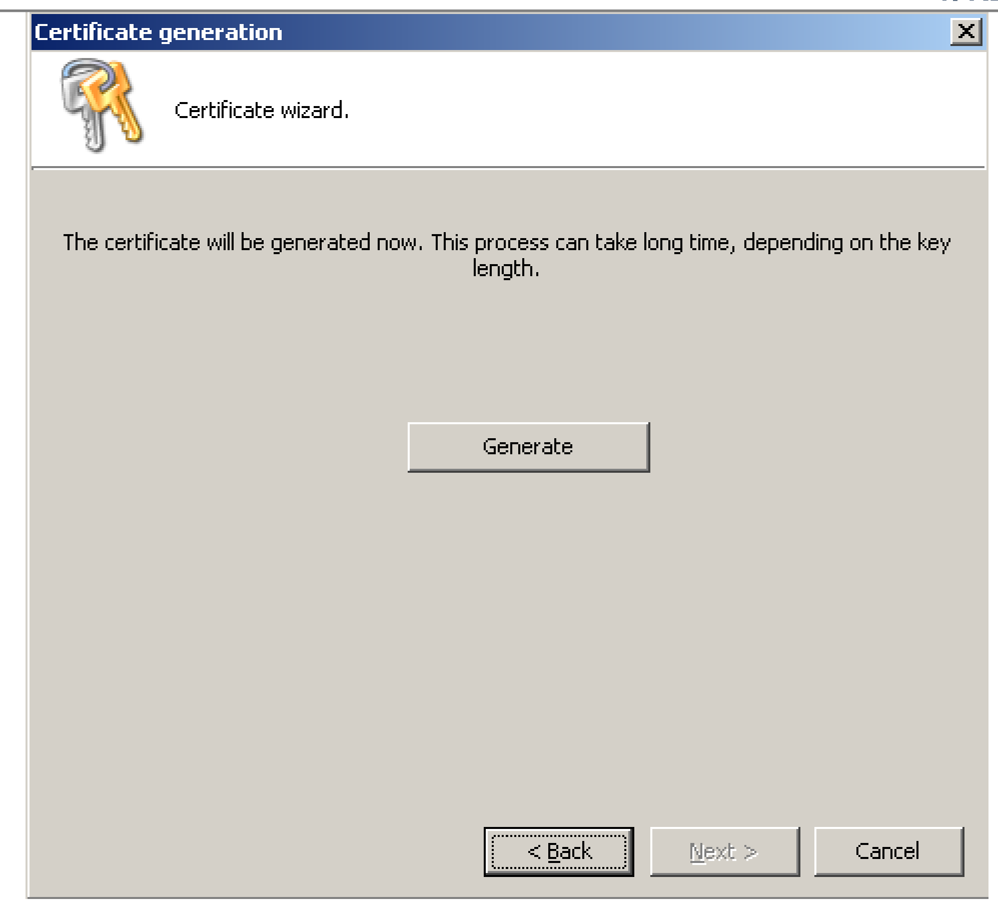



Abbildung: MailSealer – Generierung des Root-Zertifikates




## Root (CA) Zertifikat hochladen

3. *Eigenes CA Zertifikat für Ihr REDDOXX CA hochladen:*
   Fall Sie ein CA (Root) Zertifikat erworben haben, können Sie dieses auf Ihre REDDOXX hochladen. Wählen Sie dazu die entsprechende Checkbox aus und Klicken Sie auf „*LOAD*". Es erscheint folgender Dialog.

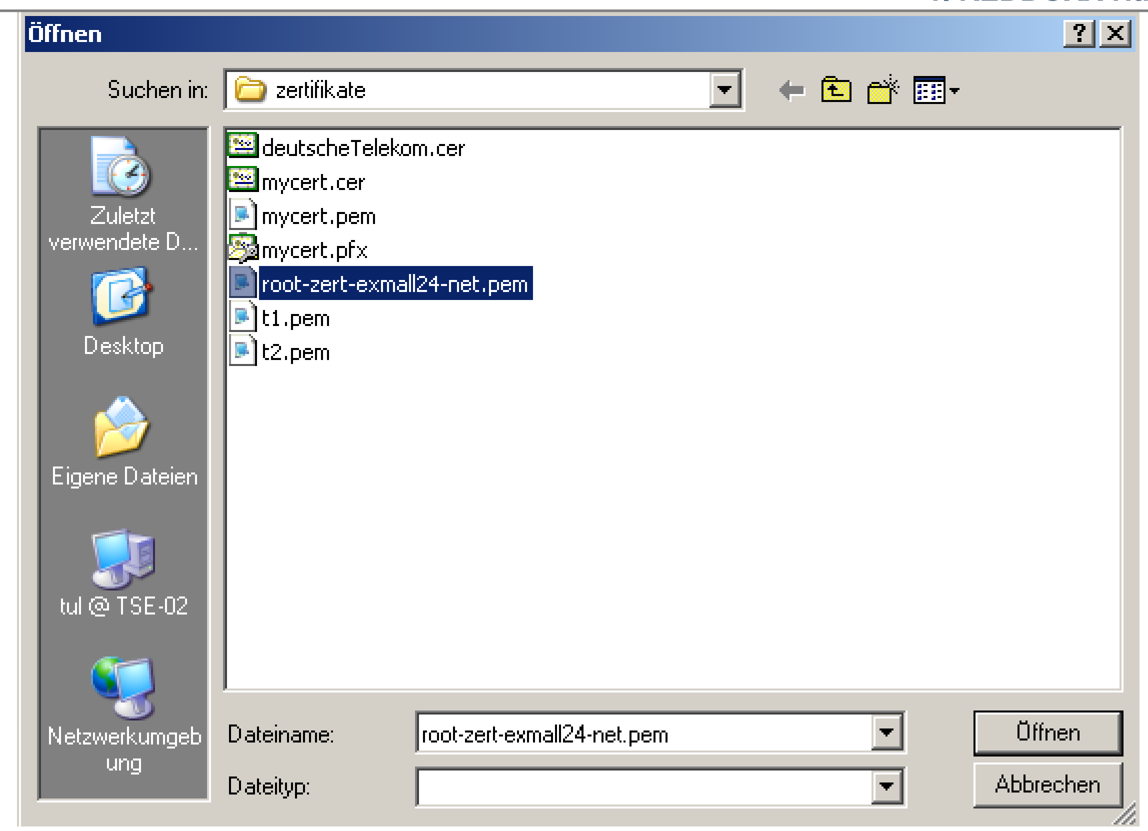



Abbildung: MailSealer – REDDOXX CA – Root Zertifikat laden – Dateiauswahl

4. Wählen Sie das gewünschte Root-Zertifikat aus und klicken Sie auf Öffnen. Es erscheint folgender Dialog.




5. Geben Sie das Passwort für den privaten Schlüssel ein und klicken Sie auf OK. Es erscheint folgender Dialog mit der Bestätigung, dass das Zertifikat erfolgreich erstellt (eingestellt) wurde.



## Selbst-Signierte personenbezogene Zertifikate hinzufügen

1. Klicken in der Menüleiste oben auf das Plus-Symbol oder klicken Sie mit der rechten Maustaste in der Listenansicht und wählen Sie „*hinzufügen*“, um eine neues Zertifikat hinzuzufügen. Folgender Dialog geht auf:

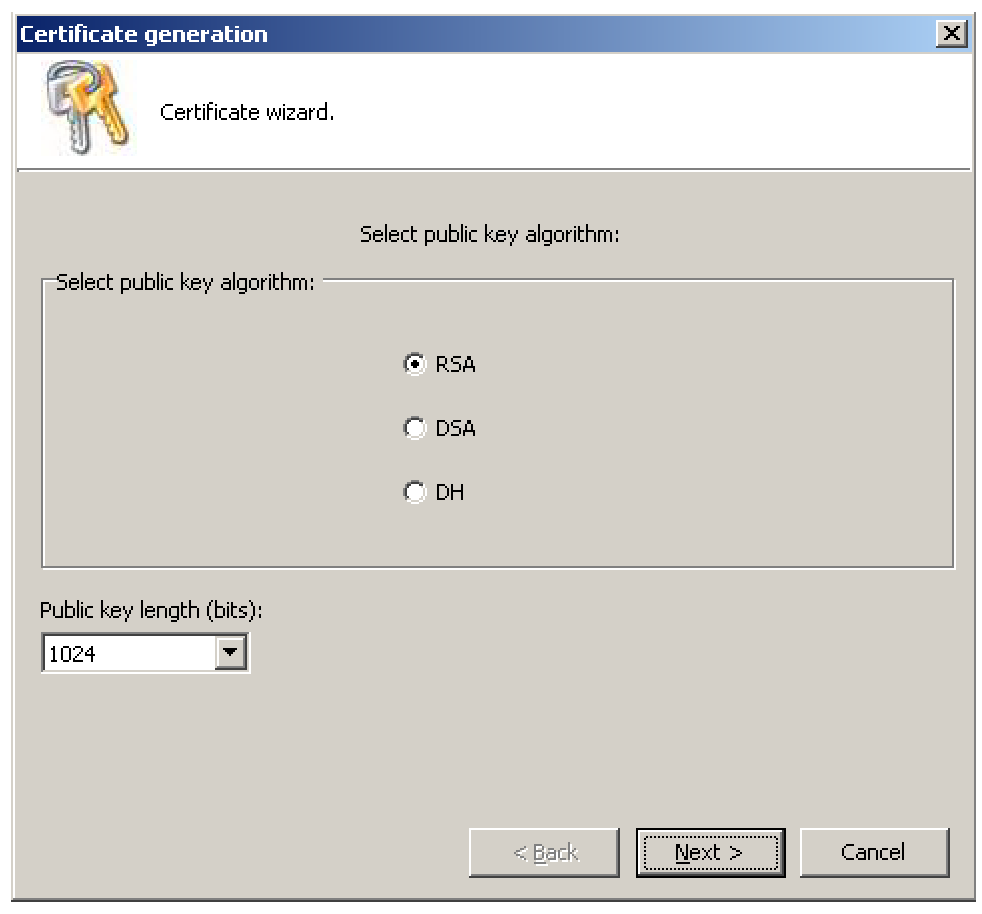



Abbildung: MailSealer – REDDOXX CA – Zertifikat erstellen – Schritt 1

2. Select public key algorithm:
   Sie haben folgende Auswahlmöglichkeiten:

   RSA : Kryptosystem nach **R**ivest, **S**hamir und **A**dleman.
   DSA: **D**igital **S**ignature **A**lgorithm. Reines Signaturverfahren der NSA.
   DH : Schlüsselaustauschverfahren nach **D**iffie-**H**ellman.

   Die Standardvorgabe ist: RSA

3. Public key length (bits): - Bitlänge des öffentlichen Schlüssels
   Der Standard ist 1024. Wählen Sie zw. 1024, 2048 und 4096 Bit.

**HINWEIS**

Je länger der Schlüssel, desto rechenintensiver (Performance) ist die kryptografische Verarbeitung (Signierung und Verschlüsselung). Je länger der Schlüssel, desto höher ist die Sicherheit.

4. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen.

**Subject Parameters - Eigenschaften des Zertifikates.**
Die Felder sind nur von beschreibender Form und haben keine weitere Funktionalität. Sie dienen zur Information und zur Überzeugung, ob dem Besitzer dieses Zertifikates vertraut werden kann.

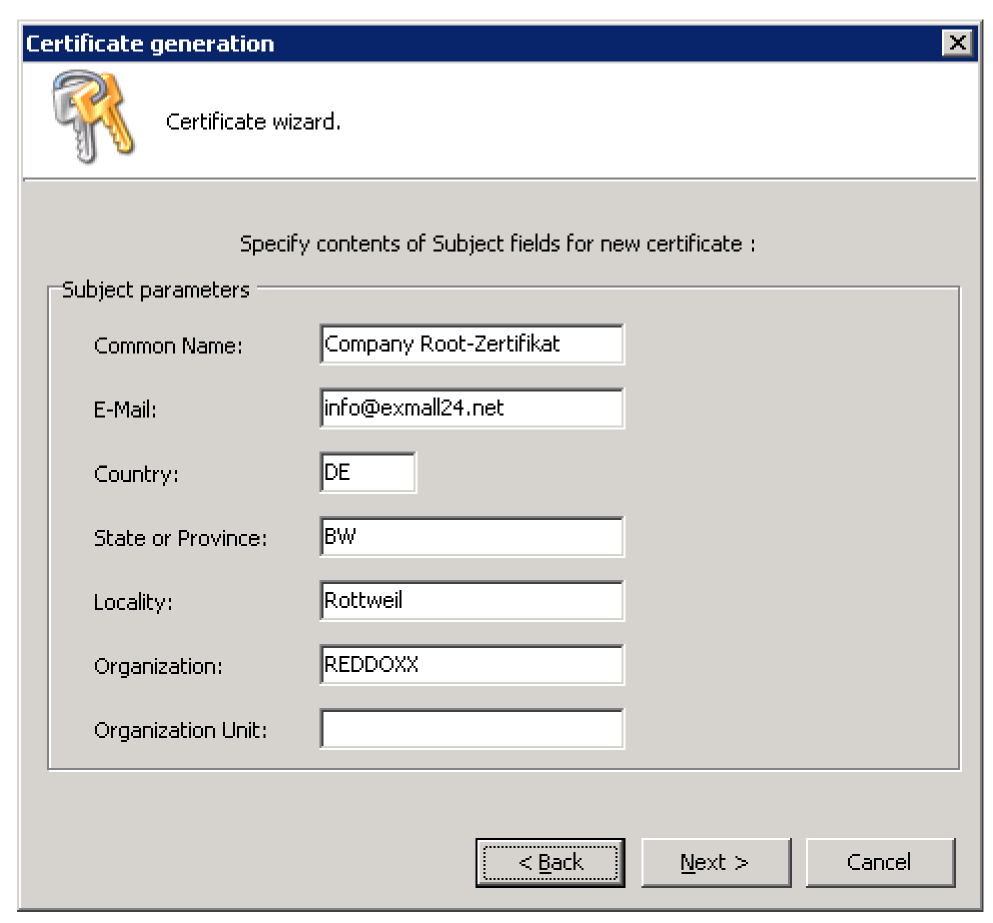



Abbildung: MailSealer – REDDOXX CA – Zertifikat erstellen - Subject-Parameter – Schritt 2

1. Common Name : Name / Bezeichnung des Zertifikates
2. E-Mail : Allgemeine E-Mail Adresse des Unternehmens
3. Country : 2 Zeichen Länder-Code (DE, US, GB, FR, ES, CH, AT, GR, AU etc.)
4. State or province : Staat, Bundesland oder Kanton.
   Beispiele: BW, Baden Württemberg, California, Uri
5. Locality : Stadt, Lokalität
6. Organization : Organisation, Einheit, Tochtergesellschaft
7. Organization Unit : Fachabteilung, Department.

8. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen, auf „BACK“ (Zurück) um zur vorhergehenden Eingabemaske zu gelangen.

**Validity period: - Gültigkeitszeitraum**
Die Felder „from“ (von) und „to“ (bis) geben den Gültigkeitszeitraum des Root-Zertifikates an. Dieser Zeitraum wird bei einer E-Mail-Verarbeitung mit überprüft, in der ein durch dieses Root-Zertifikat ausgestellte persönliches Zertifikat verwendet wird.

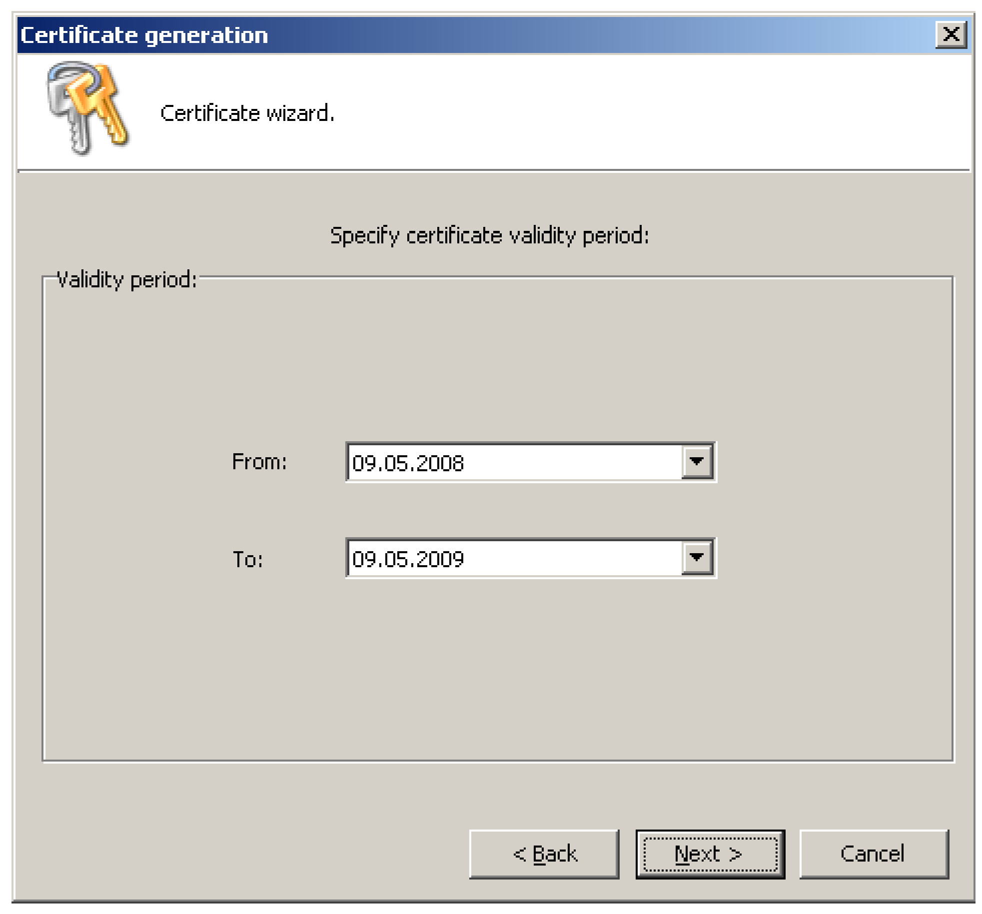



Abbildung: MailSealer – REDDOXX CA – Zertifikats-Wizard - Gültigkeitsdauer – Schritt 3

1. From (von) : Beginn des Gültigkeitszeitraumes
2. To (bis) : Ende des Gültigkeitszeitraumes

3. Drücken Sie auf „NEXT“ (Weiter) um in die nächste Eingabemaske zu gelangen, auf „BACK“ (Zurück) um zur vorhergehenden Eingabemaske zu gelangen.

4. Zertifikats-Erstellung. Mit Klick auf „GENERATE“ wird das Zertifikat erstellt. Dies dauert einen kleinen Moment (i.d.R. wenige Sekunden).

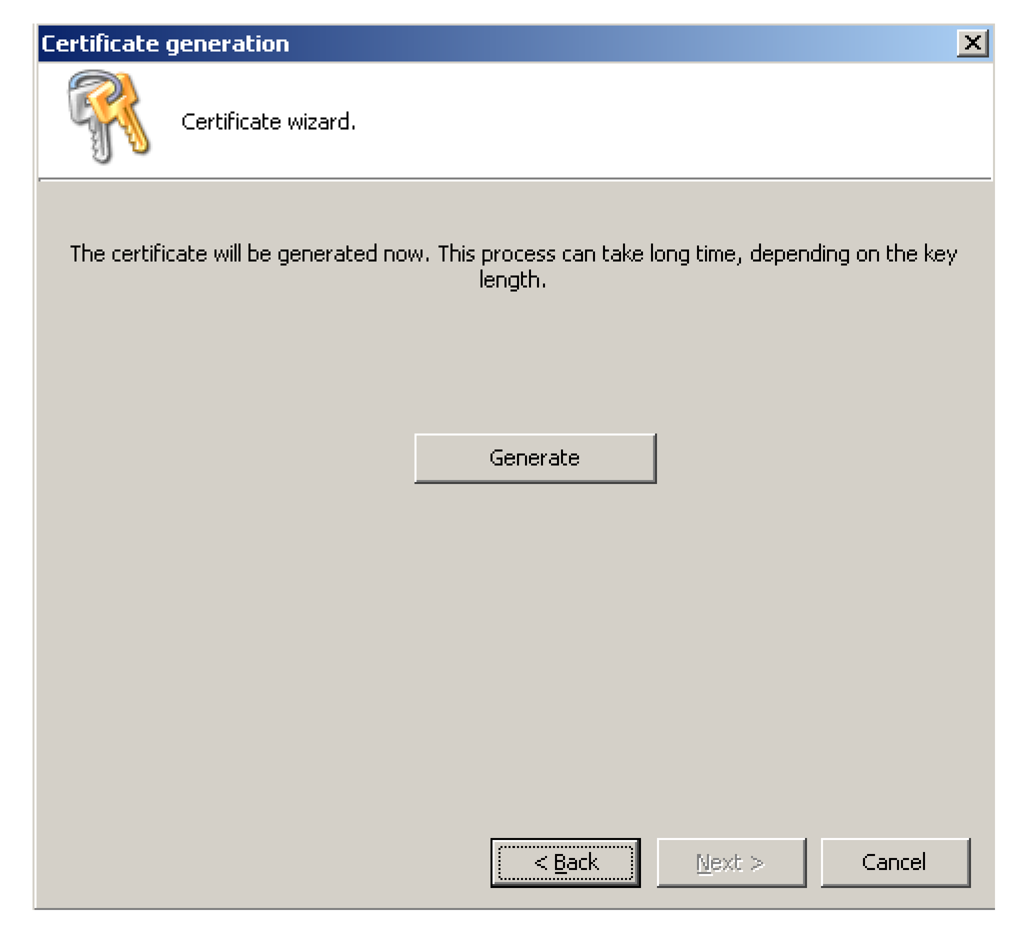
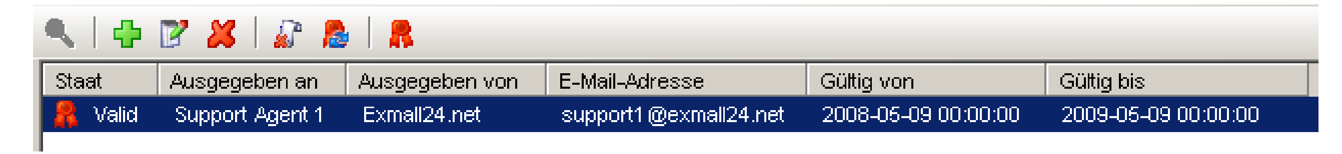



Abbildung: MailSealer – Generierung eines selbst-signierten Zertifikates

Nach erfolgreichem Generieren des Zertifikates erscheint das Zertifikat in der Listenansicht.



| Staat | Ausgegeben an | Ausgegeben von | E-Mail-Adresse | Gültig von | Gültig bis |
|---|---|---|---|---|---|
| Valid | Support Agent 1 | Exmall24.net | support1@exmall24.net | 2008-05-09 00:00:00 | 2009-05-09 00:00:00 |

Abbildung: MailSealer – Listenansicht eines selbst-signierten Zertifikates

**Funktionen im Kontextmenü**

Die Funktionen des Kontext-Menüs verhalten sich gleich wie mit denen der privaten und öffentlichen Zertifikate, wie unter Kapitel ➔4.6.8.3.1 beschrieben.

Die Funktion „Verwerfen“ (Sperren) ist bei selbst erstellten Zertifikaten innerhalb der REDDOXX CA nun möglich.

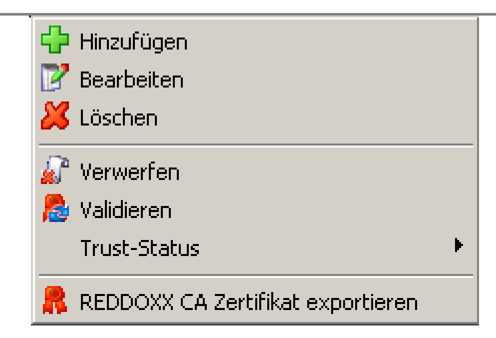



Abbildung: MailSealer – Kontextmenü eines selbst-signierten Zertifikates

**REDDOXX CA Zertifikat exportieren**
Damit Ihre selbst erstellten (selbst-signierten) Zertifikate von Ihren Kommunikationspartnern als gültig erkannt werden, ist es erforderlich, dass Sie ihnen Ihr Root (CA) Zertifikat geben. Hierzu reicht der öffentliche Schlüssel innerhalb des Zertifikates.
Den privaten Schlüssel exportieren Sie nur dann, wenn Sie dieses Root-Zertifikat auf eine andere Appliance übertragen wollen und damit sicher stellen wollen, dass die bisher mit diesem Root-Zertifikat ausgestellten persönlichen Zertifikate, weiterhin gültig sind.

1. Wählen Sie aus dem Kontextmenü der Listenansicht den Punkt *„REDDOXX CA Zertifikat exportieren“* oder klicken Sie in der Menüleiste oben auf das Symbol. Der weitere Vorgang ist identisch mit dem Export eines gewöhnlichen Root-Zertifikates wie in Kapitel ➔4.6.8.3.3 beschrieben.

# 5 POP3 und Bridge-Modus

Seit der REDDOXX Build Version 1024 können E-Mails nun auch per POP3 abgeholt werden.

## 5.1 Funktionsweise von POP3 mit REDDOXX

1. Ein Mail-Client startet mit einer POP3-Anfrage.
2. Die REDDOXX nimmt diese Anfrage entgegen und merkt sich die Login-Daten.
3. Die Appliance gibt dem Mail-Client alle E-Mails, die bereits in der Warteschlange für *„Ausgehende Nachrichten für POP3“* stehen. Die Abhol-Anfrage des E-Mail-Clients ist damit beendet.
4. Die Appliance meldet sich mit den zwischengespeicherten Login-Daten beim eigentlichen Mailbox-Provider an.
5. Sie holt alle E-Mails ab und stellt diese in die *„Eingehende Warteschlange für POP3“.*
6. Der Validierungs-Prozess der Appliance filtert den Spam heraus und archiviert die E-Mail sofern das MailDepot aktiviert ist.
7. Zuletzt wird die E-Mail in die Warteschlange für *„Ausgehende Nachrichten für POP3“* gestellt und ist zur Abholung durch den Mail-Client bereit.

HINWEIS:

Beim Abholen der E-Mails durch POP3 über die REDDOXX Appliance geschieht die Zustellung der E-Mail erst beim zweiten Abruf durch den Mail-Client.

**Beispiel:**

Abholung der E-Mails erfolgt alle 5 Minuten durch den Mail-Client.

Erst nach 10 Minuten erreicht die eigentliche E-Mail den Mail-Client, da die E-Mail auf der REDDOXX zwischengepuffert und validiert wird.

**CISS:**
Beachten Sie dabei auch, dass durch dieses Prinzip bedingt, eine CISS-Challenge erst dann zum Absender gesendet wird, wenn die E-Mail vom POP-Client abgeholt wird. Bei einem zentralen POP3-Abholdienst (z.B. fetchmail, POPCon etc.) stellt dies kein Problem dar. Lediglich beim Abholen durch einzelne Mail-Clients (z.B. nach Rückkehr des Benutzers aus dem Urlaub), wird die CISS-Challenge generiert.

## 5.2 Betriebsarten

Das Abholen von E-Mails via POP3 kann in zwei verschiedenen Modi betrieben werden, im Standard- und im Bridge-Modus.

## 5.2.1 Standard-Modus

Im Standard-Modus wird die REDDOXX Appliance mit einem LAN-Interface (LAN-1) angeschlossen.

### 5.2.1.1 Konfiguration für den Mailempfang via POP3

Konfigurieren Sie die Zugangsdaten zu Ihrer Pop3-Mailbox in Ihrem Mail-Client wie nachfolgend beschrieben. Achten Sie dabei auf die abgeänderte Form des Kontonamens.

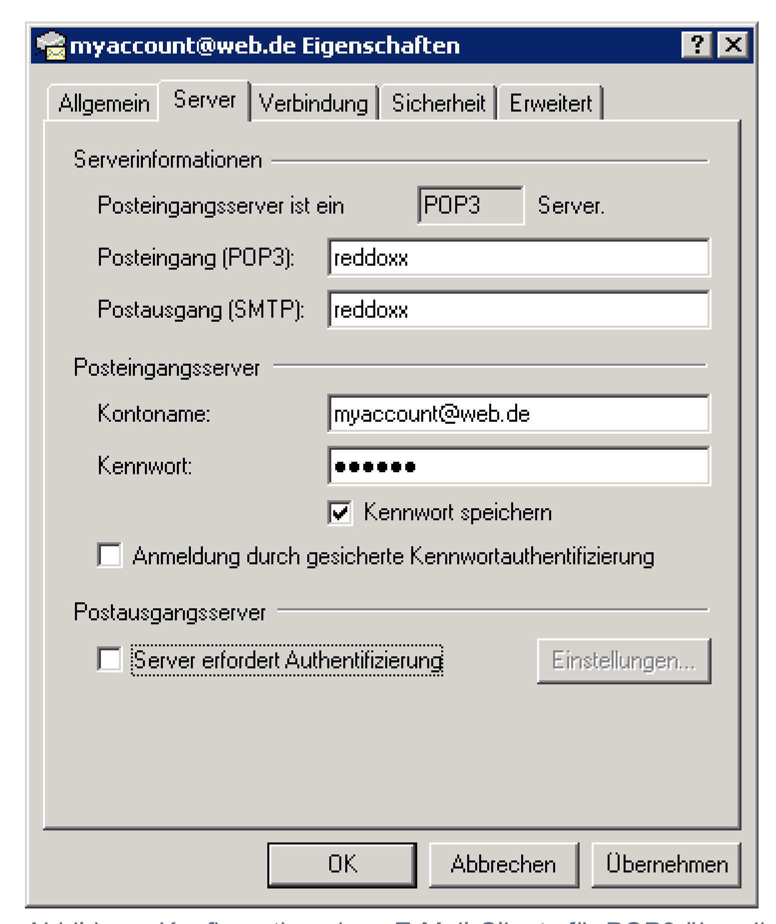



Abbildung: Konfiguration eines E-Mail-Clients für POP3 über die REDDOXX.

**Posteingangsserver**

Posteingang : Hostname oder IP-Adresse Ihrer REDDOXX-Appliance.

Kontoname : Der Kontoname wird aus dem eigentlichen Login plus dem Hostnamen des POP3-Servers Ihres Providers zusammengesetzt.

BEISPIEL

Ihre E-Mailadresse lautet: myaccount@web.de
Der Login lautet: myaccount
Der Pop3-Server heißt: pop3.web.de

Daraus ergibt sich der neue Kontoname: **myaccount@pop3.web.de**

Verwenden Sie nun diesen zusammengesetzten Kontonamen zur POP3-Anmeldung an Ihrer REDDOXX-Appliance.

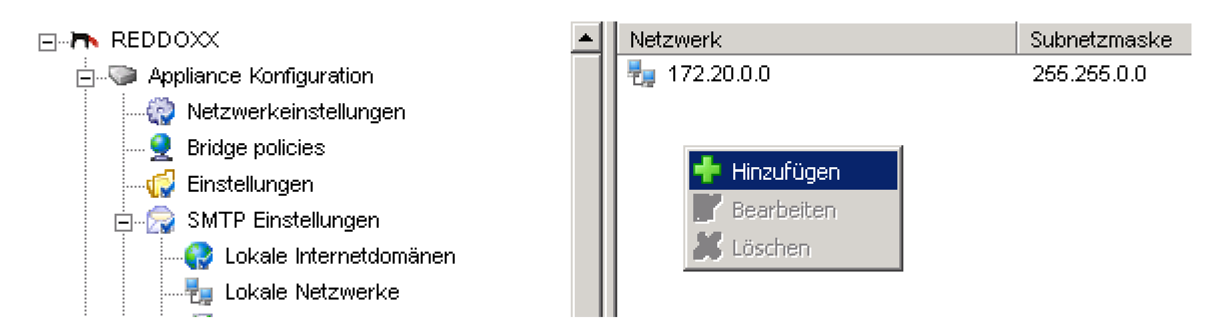
**Postausgangsserver**
Server erfordert Authentifizierung: Diese Option darf nicht gesetzt sein!

HINWEIS:

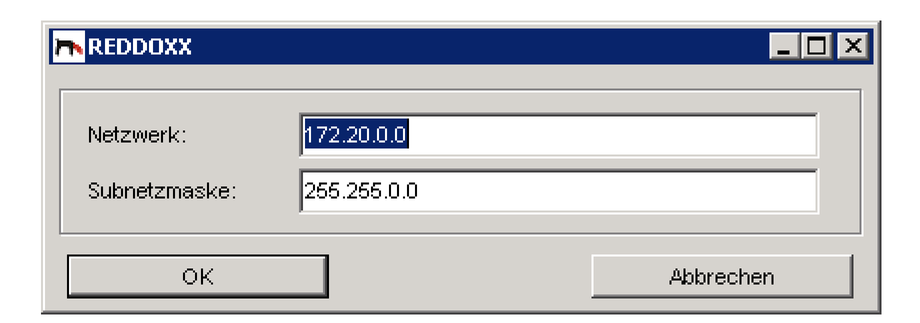
Beim Abholen der E-Mails durch POP3 über die REDDOXX Appliance werden die E-Mails immer auf dem Mail-Server gelöscht, unabhängig davon, ob Sie die Option „Mail auf dem Server nicht löschen" gesetzt haben, oder nicht!

### 5.2.1.2 Konfiguration für den Mailversand via SMTP

**Lokale Netzwerke - Berechtigung zum Versand**
Für den Mailversand ist es erforderlich, dass die sendenden Stationen auf der REDDOXX Appliance freigeschalten sind. Sie können dies in den SMTP-Einstellungen – Lokale Netzwerke - konfigurieren.




Fügen Sie das Netzwerk hinzu, für das Sie den SMTP-Versand auf der REDDOXX erlauben möchten. Einzelne Stationen (IP-Adressen) kennzeichnen Sie in der Subnetzmaske für Angabe von 255.255.255.255




Starten Sie danach den SMTP-Server Dienst neu.

**Mailversand über ein Relay**
Verfügen Sie nicht über eine feste IP-Adresse, muss die REDDOXX E-Mails ins Internet über ein Mail-Relay versenden. Tragen Sie unter *EINSTELLUNGEN*, wie im

nachfolgenden Bild beschrieben, das Relay ein, das Sie von Ihrem Telekommunikationsprovider erhalten haben.

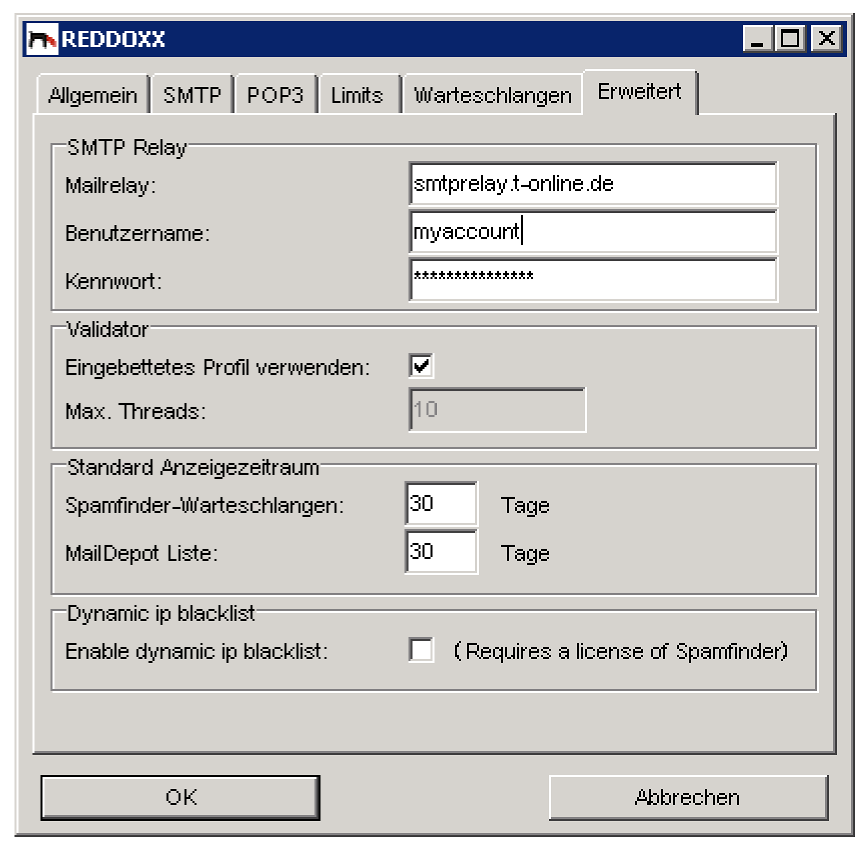



Abbildung: Konfiguration des Relays.

### 5.2.1.3 Konfiguration der lokalen Internetdomänen

**Lokale Internetdomänen für die Archivierung**

Damit ausgehende E-Mail archiviert werden können, ist es erforderlich, dass die Absender-Adress-Domäne in den lokalen Internetdomänen eingetragen wird.

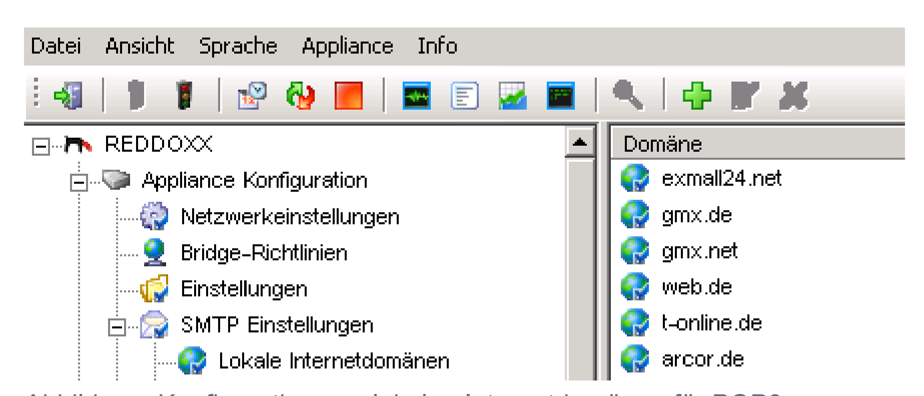



Abbildung: Konfiguration von lokalen Internetdomänen für POP3

HINWEIS:

Falls Sie neben Ihrer eigenen Internetdomäne auch E-Mailadressen von Providern nutzen, müssen Sie, damit ausgehende E-Mails ebenfalls archiviert werden können, diese Domänen eintragen.

## 5.2.2 Bridge-Modus

Im Bridge-Modus wird die REDDOXX Appliance zwischen Firewall und dem LAN (i.d.R. ein Switch) geschaltet, sodass der komplette Internetverkehr durch die REDDOXX Appliance fließt.
Der Vorteil des Bridge-Modus ist, dass Ihre vorhandene Infrastruktur sowohl für das Abholen Ihrer Mails via POP3, als auch für den Versand via SMTP nicht angepasst werden muss.

### 5.2.2.1 Konfiguration und Aktivierung des Bridge-Mode

Schließen Sie zunächst die Appliance, wie im Standard-Modus beschrieben, über das LAN-1 Interface an. Verbinden Sie sich mit der Adminkonsole auf Ihre Appliance und aktivieren Sie den Bridge-Mode unter den *Netzwerkeinstellungen*.



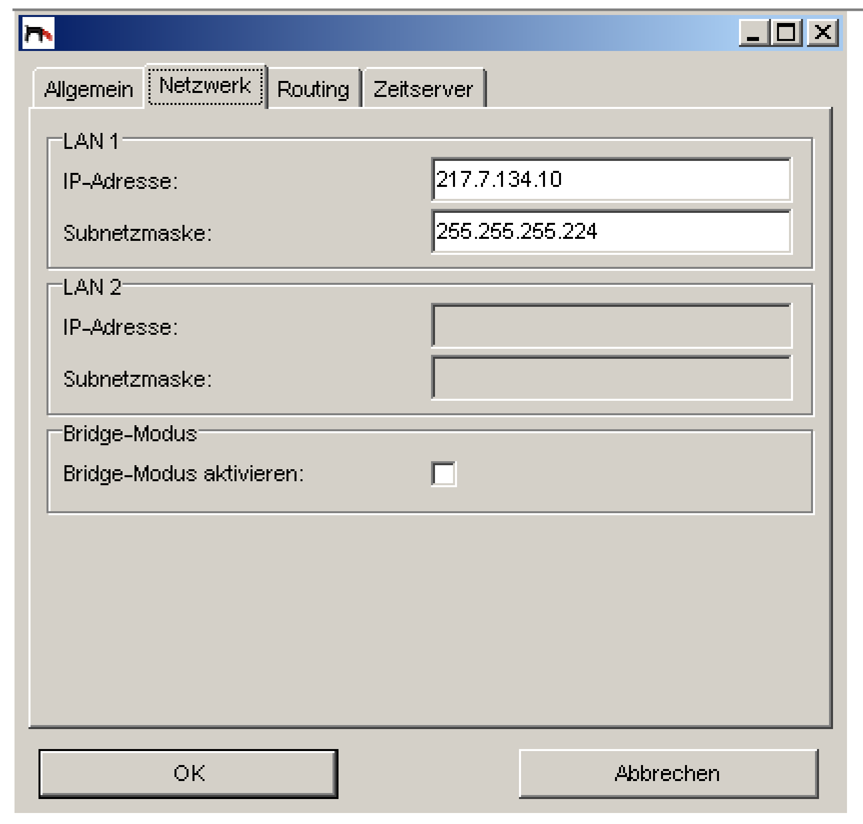



Abbildung: Netzwerkkonfiguration – Aktivierung des Bridge-Modus

Danach muss die Reddoxx neu gestartet werden. Wählen Sie im Menü *Appliance – Neu Starten* aus.
Im aktivierten Bridge-Mode werden die TCP-Verbindungen der Ports für SMTP (25), POP3 (110) und POP3s (995) abgefangen und von der REDDOXX Appliance weiterverarbeitet. Alle anderen Protokolle werden unverändert durchgeleitet.

### 5.2.2.2 Anschluss der Appliance für den Bridge Betrieb

Im Bridge-Modus wird die Appliance physikalisch zwischen dem Internet-Gateway (Firewall/Router) und dem nachfolgenden Switch geschaltet. Sie verbinden den Gateway mit der LAN Buchse 1 und das nachfolgende LAN (Switch) mit der LAN Buchse 2.
Bedenken Sie, dass dabei die Internetverbindung kurzzeitig unterbrochen wird.
Der gesamte Internetverkehr wird jetzt durch die Appliance geleitet.

**HINWEIS**

Verwenden Sie beim Verbinden der Appliance mit der Firewall unbedingt ein Cross-Kabel.

### 5.2.3 Bridge Richtlinien

In der Appliance Konfiguration finden Sie den Punkt Bridge Richtlinien. Hier können Sie Regeln definieren, die bestimmte Teilnehmer (Mail-Clients) oder Internet-Mail-Server vom Proxy-Betrieb ausschließen. Das bedeutete dass der Internetverkehr für diese Teilnehmer einfach unberücksichtigt und unverändert durchgeschleust wird.

.

1. Klicken Sie doppelt auf die *Bridge Richtlinien*.
   Folgende Felder werden angezeigt:

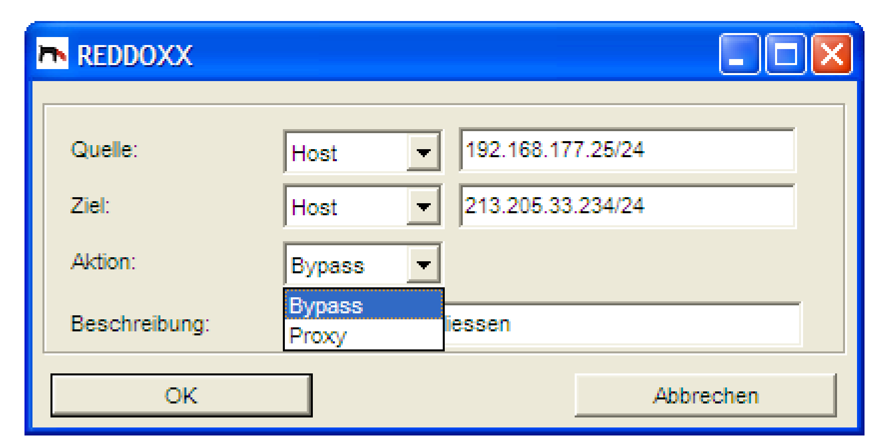



Abbildung: Bridge Richtlinien der REDDOXX Appliance

2. *Quelle*: ist ein Client im internen Netz, alle oder ein bestimmtes Netzwerk
3. *Ziel*: ist der Provider dessen IP Adresse hier eingetragen wird, alle, oder ein bestimmtes Netzwerk
4. *Aktion:* *„Bypass"* - die Mails werden nicht von der Reddoxx abgeholt, sondern vom Client beim Provider.
   *„Proxy"* – die Mails werden zuerst von der Reddoxx abgeholt, anschließend vom Client.

Sie haben durch die Richtlinien die Möglichkeit verschiedene Regeln zu kombinieren. Die Verarbeitung der Regeln läuft von oben nach unten. Sobald eine Regel zutrifft, wird diese angewendet. Weitere nachfolgende Regeln werden nicht mehr berücksichtigt.



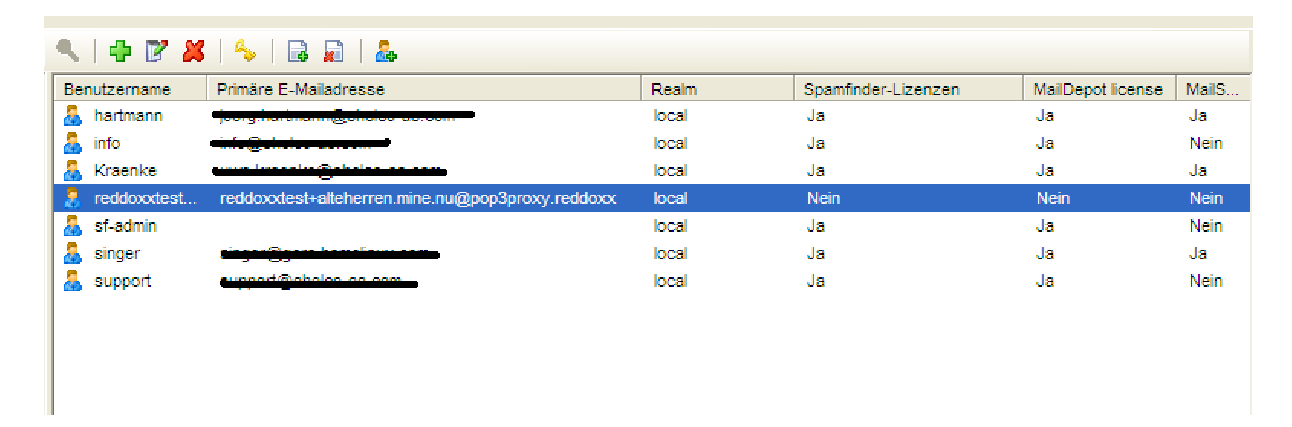
**HINWEIS**

Veränderte Regeln werden erst nach dem Drücken des Aktivieren-Symbols ✔ in der Symbolleiste wirksam.

## 5.3 Benutzer verwalten

Das Anlegen der User und der E-Mail-Aliase geschieht automatisch sobald ein Client eine E-Mail von seinem Provider abruft.

Der E-Mail-Alias erhält dabei die Pseudo-Domäne *pop3proxy.reddoxx (siehe nachfolgende Abbildung).* Lizenzen werden automatisch zugeteilt, sofern noch welche verfügbar sind.




**HINWEIS**

Beachten Sie beim Betrieb von Sammel-Mailboxen, dass die einzelnen E-Mail-Adressen alle einem einzigen Benutzer (Login) zugeordnet sind. Analog dazu wird auf der REDDOXX Appliance auch nur ein Benutzer angelegt und ihm alle E-Mail-Aliase zugeordnet. Die Warteschlangen können folglich auch nur von diesem einen Benutzer (Login) verwaltet werden.

Lösung:
Gewünschte Benutzer lokal anlegen und die E-Mail-Adressen einzeln zuweisen.

**Archivierung ausgehender E-Mails**

Damit der Benutzer auch seine ausgegangenen E-Mails im Archiv sehen kann, muss die E-Mail-Adresse den Benutzer manuell zugeordnet werden. Beachten Sie dabei auch, dass die Domäne dieser E-Mailadresse  unter *lokalen Internetdomänen* eingetragen ist.

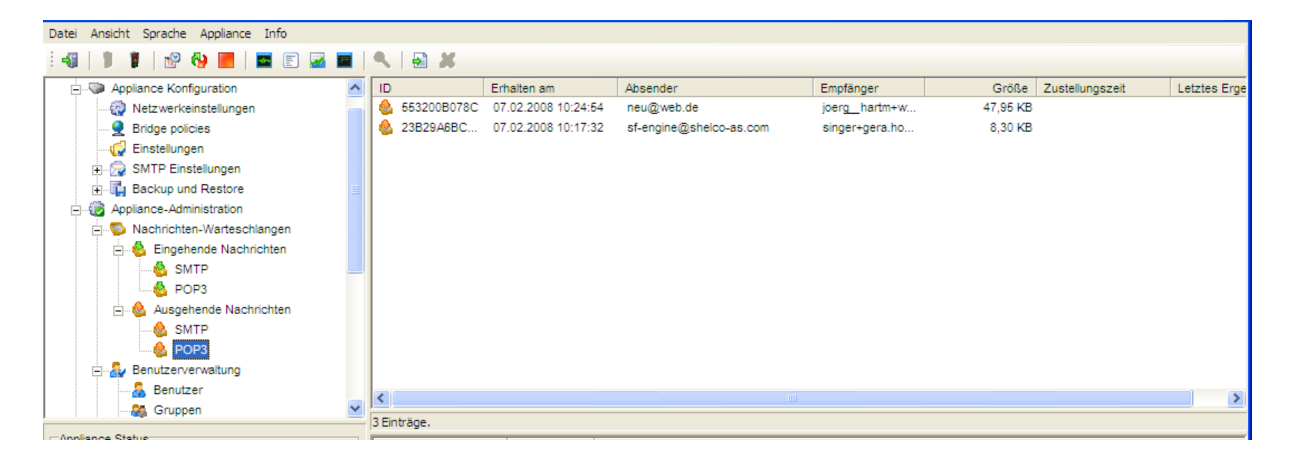
### 5.3.1 Login an der Userkonsole

Beim Anmelden an der User-Konsole wählen Sie den Benutzernamen, den Sie auch für den POP3-Login angeben haben.
Achten Sie darauf, dass ein „@“ im Benutzernamen durch ein „+“ ersetzt werden muss.
Das Passwort ist genau das gleiche, das Sie bei Ihrem Provider verwenden.




### 5.3.2 Nachrichten Warteschlangen

In der *Appliance-Administration → Nachrichten Warteschlangen* sehen Sie ob sich eine Nachricht noch in der Appliance befindet. Unter -*Eingehende Nachrichten-POP3* können Sie die Nachrichten sehen die von der Reddoxx abgeholt wurden aber noch nicht verarbeitet wurden. Unter -*Ausgehende Nachrichten-POP3* sehen Sie die Nachrichten die von der Reddoxx verarbeitet wurden aber noch nicht von einem Client abgeholt wurden.




# 6 Die Appliance-Konsole

**Allgemein**
Die Appliance – (oder auch Terminal) -Konsole ist für systemnahe Konfigurations- und Wartungsarbeiten, wie z.B. Netzwerkeinstellungen, Datensicherung und Wiederherstellung, sowie der Start und Stop von versch. Services vorgesehen.

**Verbindung zur Appliance Konsole**

Die Appliance Konsole ist über das Terminal (direkt angeschlossener Monitor) oder via SSH (z.B. Putty) erreichbar. Melden Sie sich als Benutzer „admin“ mit Passwort „AppAdmin“ an.

**Funktionsüberblick**

Die Appliance-Konsole beinhaltet folgende Funktionsmöglichkeiten.

- Initiale Netzwerkeinstellungen für die sofortige Erreichbarkeit im Netzwerk.
- System- und Datensicherung (Backup und Restore).
- Zurücksetzen des Appliance zum Ursprungszustand (Factory Settings).
- Clusterverwaltung
- Maildepot löschen und Neuindizierung
- Starten u. Stoppen des Remote Support Services und der Appliance.
- Anpassen des Admin-Passworts für diese Appliance Konsole.

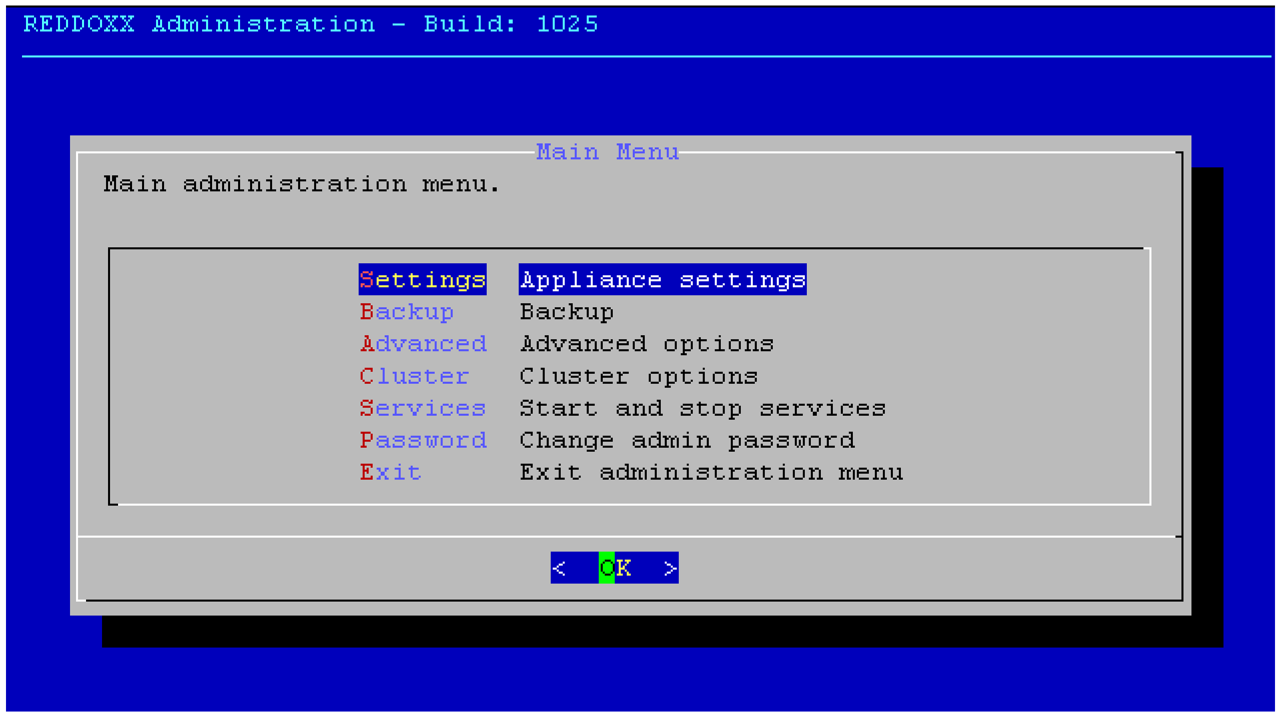
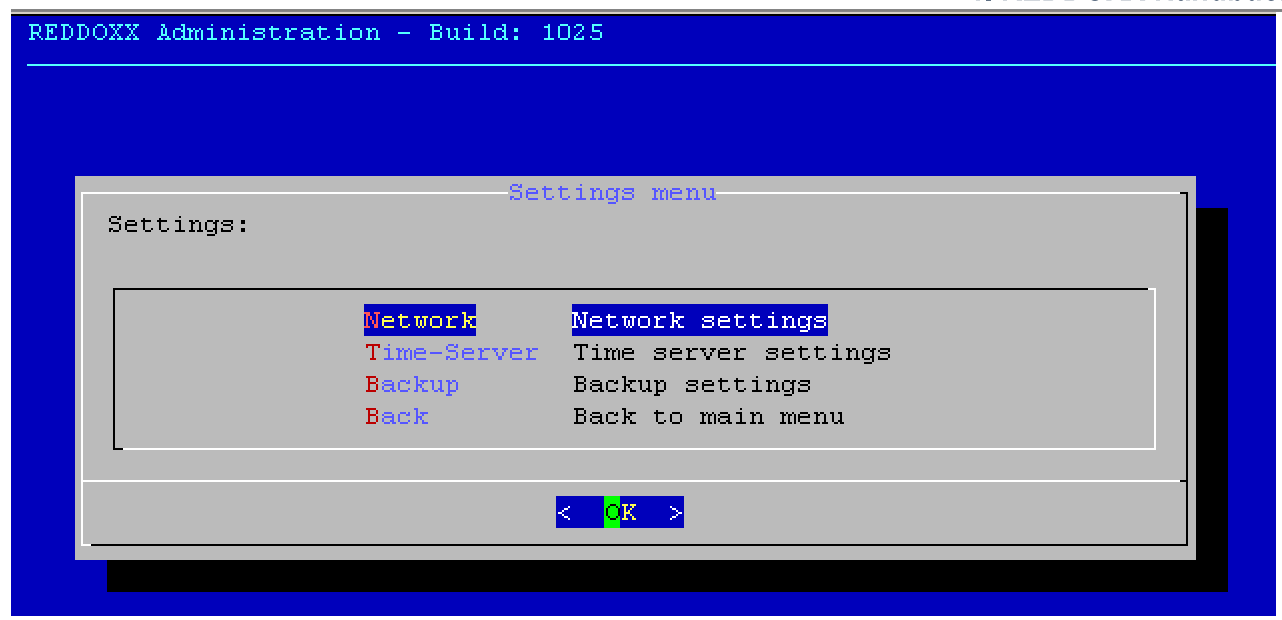



Abbildung: Hauptmenü Appliance Konsole

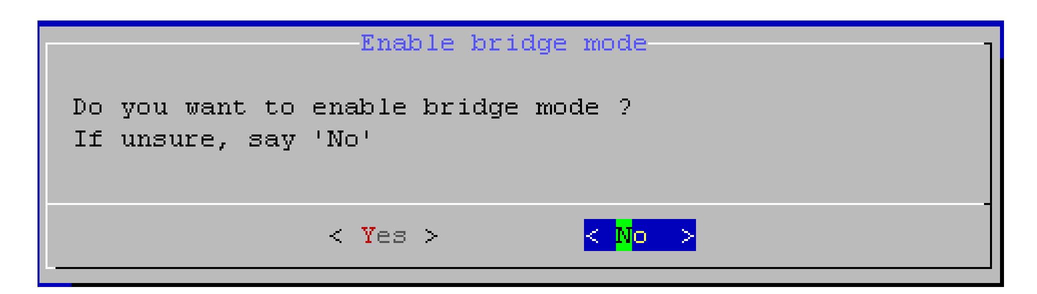
## 6.1 Appliance Settings

In den Appliance Settings können die Netzwerkkonfiguration vornehmen, Zeitserver setzen, sowie die Grundeinstellungen für ein Backup und Restore vornehmen.

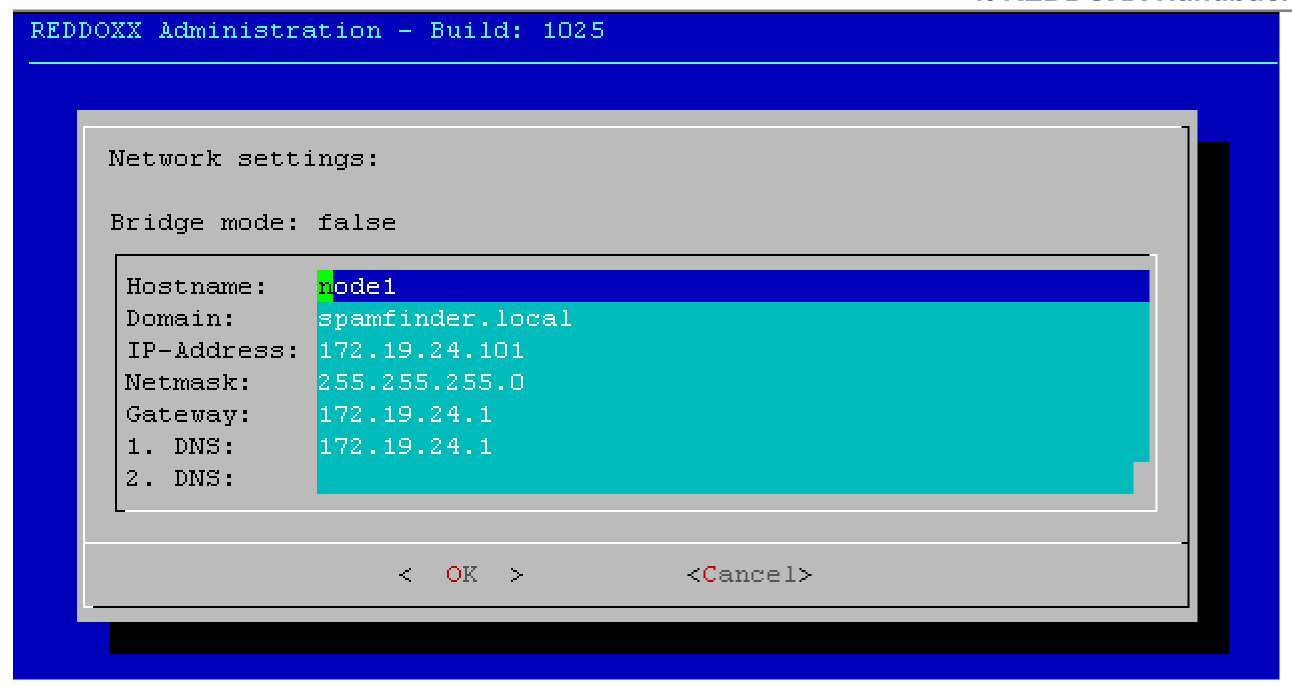



### 6.1.1 Network Settings

Zuerst werden Sie gefragt, ob Sie den Bridge Modus aktivieren wollen.

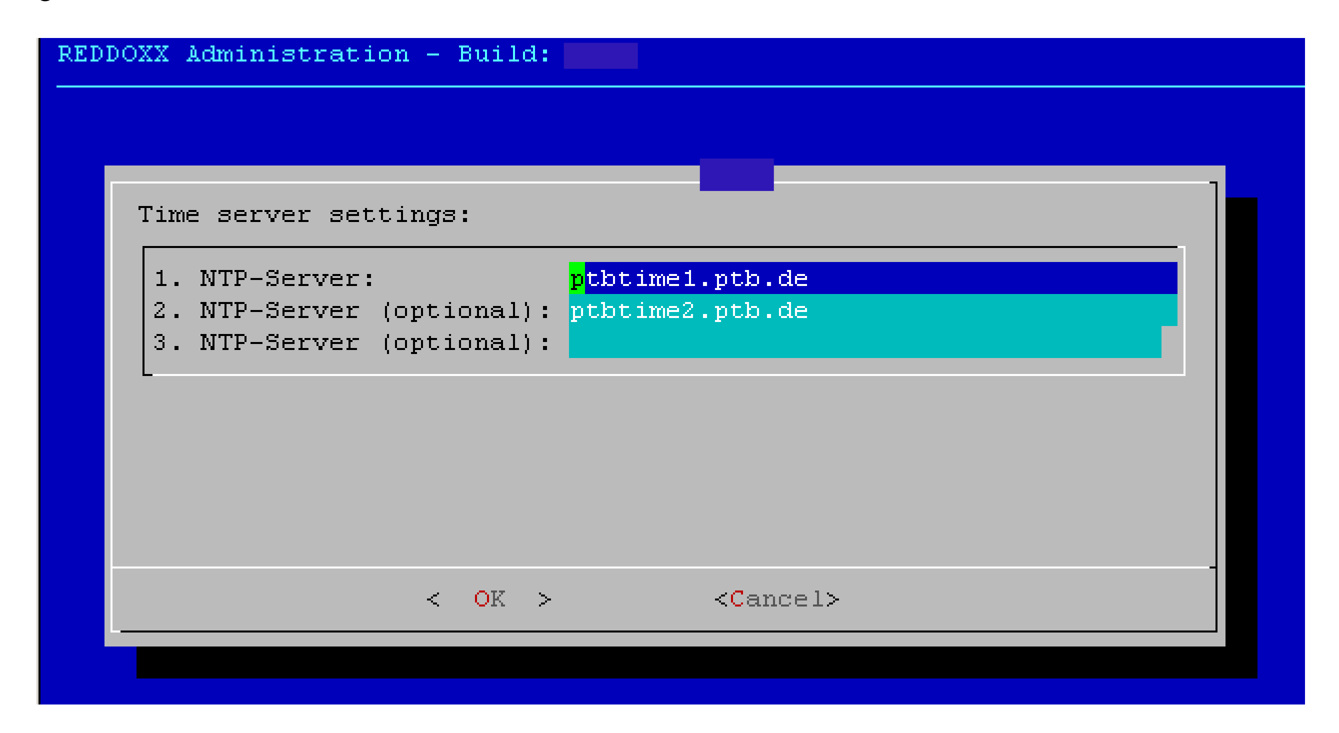



Stellen Sie dann die Netzwerkparameter ein für Hostnamen, Domainnamen, IP-Adresse, Netzmaske, Gateway und zwei DNS-Server. Wählen Sie OK. Das Netzwerk wird neu gestartet und ist sofort unter den neuen Angaben einsatzbereit.


REDDOXX Administration - Build: 1025
Network settings:
Bridge mode: false
Hostname: node1
Domain: spamfinder.local
IP-Address: 172.19.24.101
Netmask: 255.255.255.0
Gateway: 172.19.24.1
1. DNS: 172.19.24.1
2. DNS:
< OK >
<Cancel>

### 6.1.2 Time Server Settings

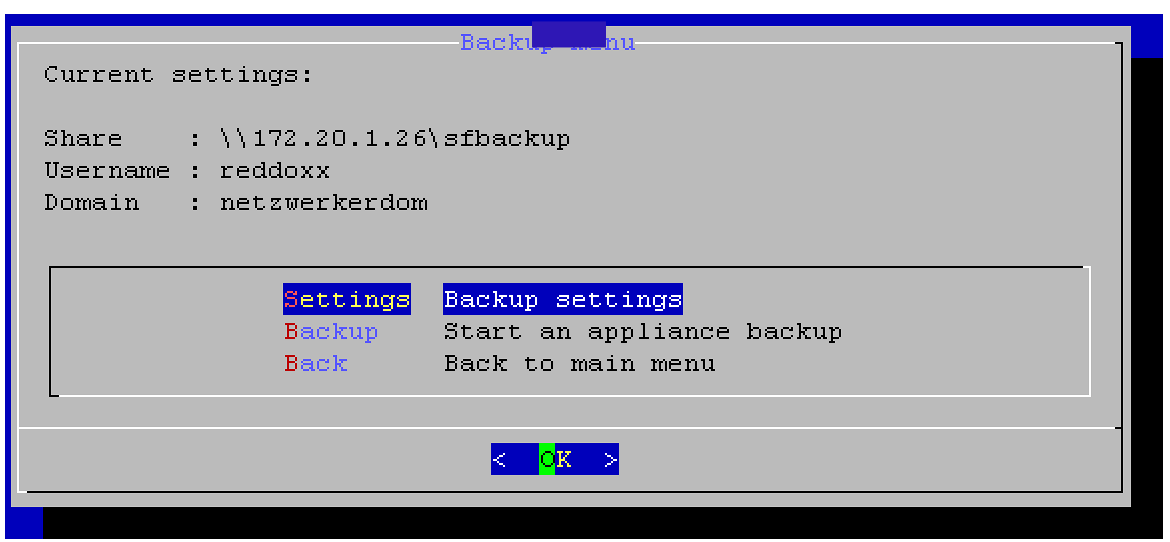
Stellen Sie hier die Zeitserver ein. Achten Sie darauf, dass der UDP Port 123 nach außen geöffnet ist.




### 6.1.3 Backup and Restore Settings

Bitte lesen Sie dies im Kapitel 6.2.1 nach.

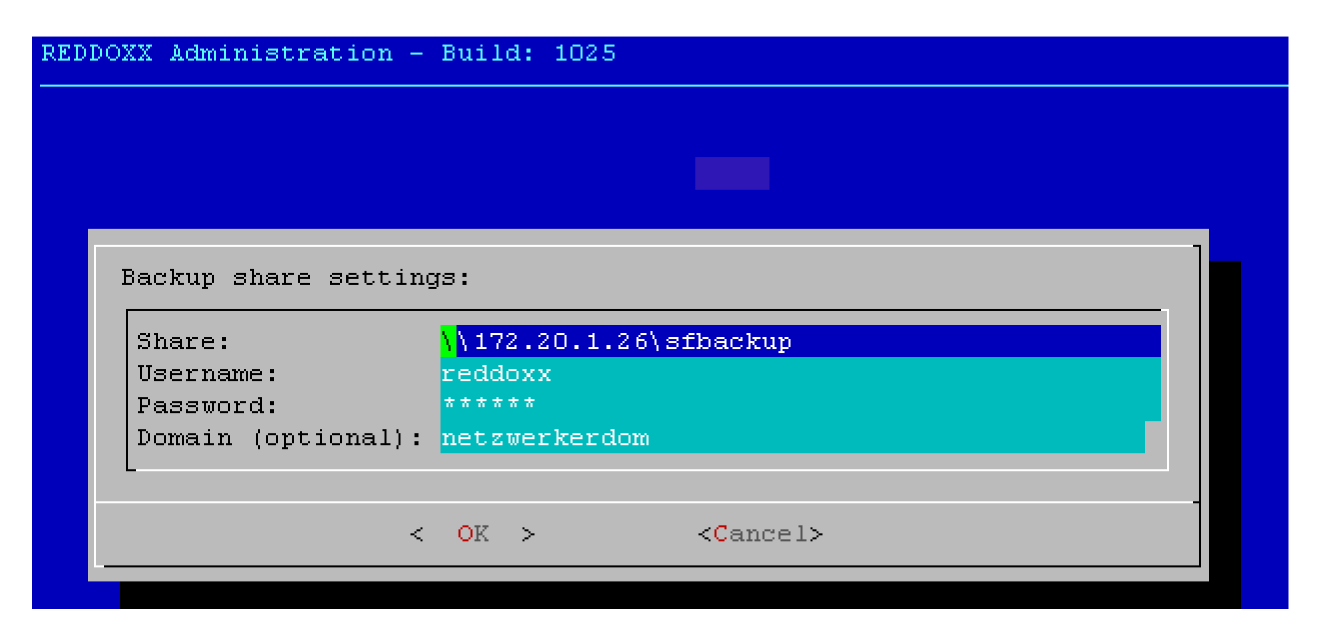
## 6.2 Backup and Restore



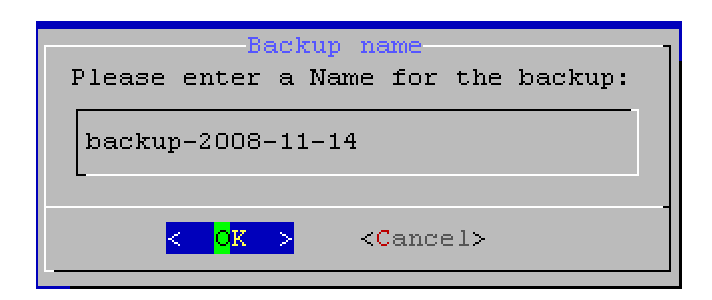

### 6.2.1 Backup and Restore Settings

Stellen Sie hier die Parameter für das Backup ein.

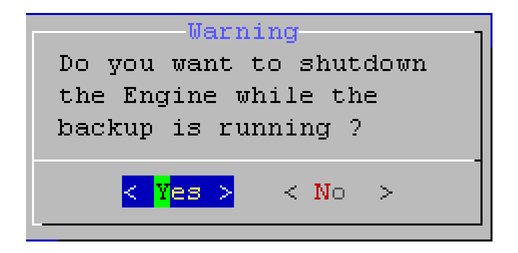
UNC-Sharename, ohne Unterverzeichnisse, Benutzername und Passwort sowie eine Domäne für die Authentifizierung an einem Domänencontroller, sofern vorhanden.




## 6.2.2 Start an Appliance Backup




Wenn Sie die Appliance auf eine andere Hardware umziehen möchten, brauchen Sie dafür einen konsistenten Zustand. Beenden Sie mit ***YES*** die REDDOXX-Engine, um dies zu gewährleisten. Der Betrieb der REDDOXX wird angehalten.
***NO***: Der Betrieb der REDDOXX wird nicht unterbrochen. Das Backup läuft im Hintergrund.



### 6.2.3 Start an Appliance Restore

Um eine Appliance zurückzusichern, starten Sie die Appliance neu und wählen Sie im Bootmenü die Option: „Appliance recovery“.

```
Normal appliance start
Appliance recovery
Memory test

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

Nach dem booten im recovery mode wird der Login angezeigt.

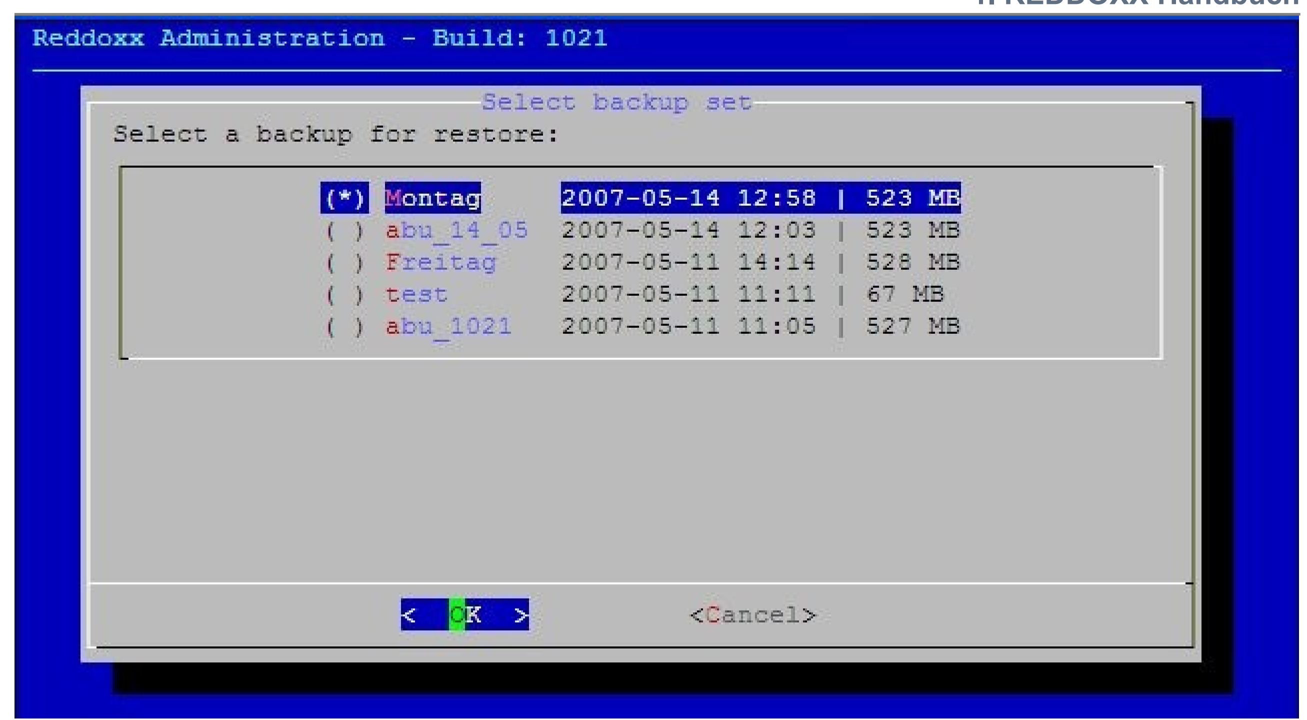
```
Appliance (recovery system) is running on: 172.19.24.102

node2 login: admin_
```

Melden Sie sich als „*admin*“ an. Das Passwort lautet „*AppAdmin*“.
Es erscheint das Hauptmenü.




Wählen Sie die Option „Restore“ aus.
Es wird eine Auswahl der vorhandenen Backups angezeigt. Wählen Sie mit den Cursor-Tasten das gewünschte Backup aus und aktivieren Sie es für das RESTORE mit der Leer-Taste (Space). Die Markierung zeigt dann einen Stern (*) an.




Bestätigen Sie die Sicherheitsabfrage mit YES. Der RESTORE startet.

Warning

Do you want to restore the following backup-set ?

Montag | 2007-05-14 12:58 | 523 MB

< Yes > < No >

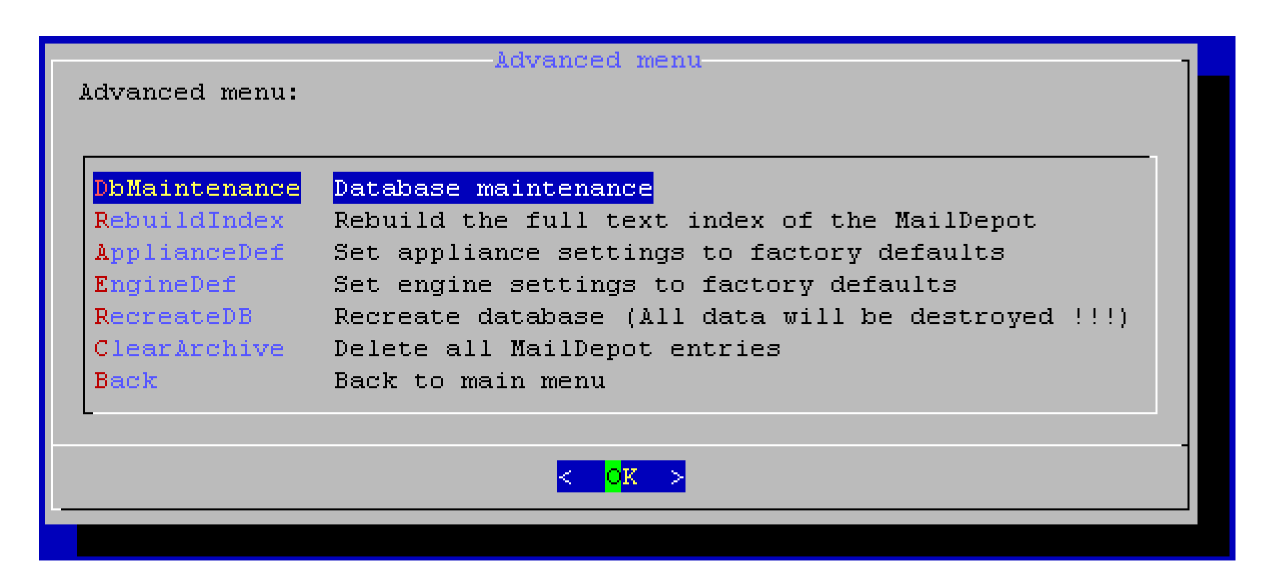
Nach erfolgreichem Zurücksichern erscheint ein Dialog, den Sie mit OK bestätigen. Starten Sie die Appliance nun neu (Reboot) im normalen Modus (Normal Appliance Start).

## 6.3 Advanced Options

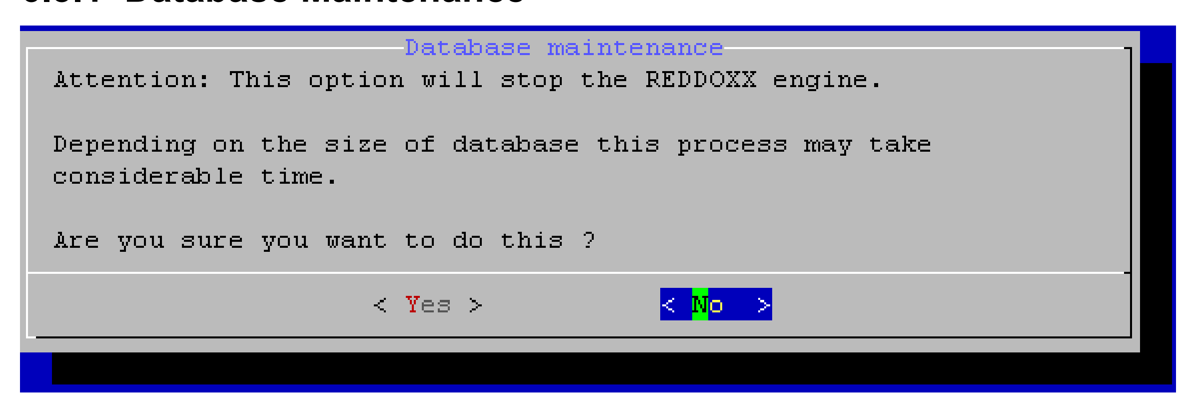
In den ADVANCED OPTIONS können Sie die Appliance auf Ihren originalen Auslieferungszustand zurücksetzen (Factory Default Settings). Darüber hinaus können Sie gezielt das MailDepot löschen oder den Index für die Volltextsuche im MailDepot neu aufbauen.

**WARNUNG**

**Beim Zurücksetzen der Appliance werden Ihre Daten gelöscht. Diese sind unwiederbringlich verloren. Nur mit einem vorhandenen BACKUP können Daten wiederhergestellt werden.**




### 6.3.1 Database Maintenance




Starten Sie die Datenbank-Reorganisation mit „Yes“, wenn Sie den Eindruck haben, dass Ihre Appliance zu langsam läuft. Bei der Reorganisation werden die Daten in der Datenbank optimiert, was sich positiv auf die Verarbeitungsgeschwindigkeit der Appliance auswirken kann.

Es erscheint folgende Anzeige.

```
Database maintenance
Stopping engine ...
Backup database ...
Restore database ...
Activate new database ...
Starting engine ...

gbak:    restactivating and creating deferred index IDX_SF_BAYES_PROBABILITY
  gbak:    activating and creating deferred index IDX_SF_BAYES_SPAMCOUNT
  gbak:    activating and creating deferred index IDX_SF_BAYES_WORD
  gbak:    activating and creating deferred index FK_MESSAGE_ID
  gbak:    activating and creating deferred index FK_USER_ID
  gbak:    committing metadata
  gbak:finishing, closing, and going home
```

Beenden Sie die Reorganisation mit der Auswahl EXIT.

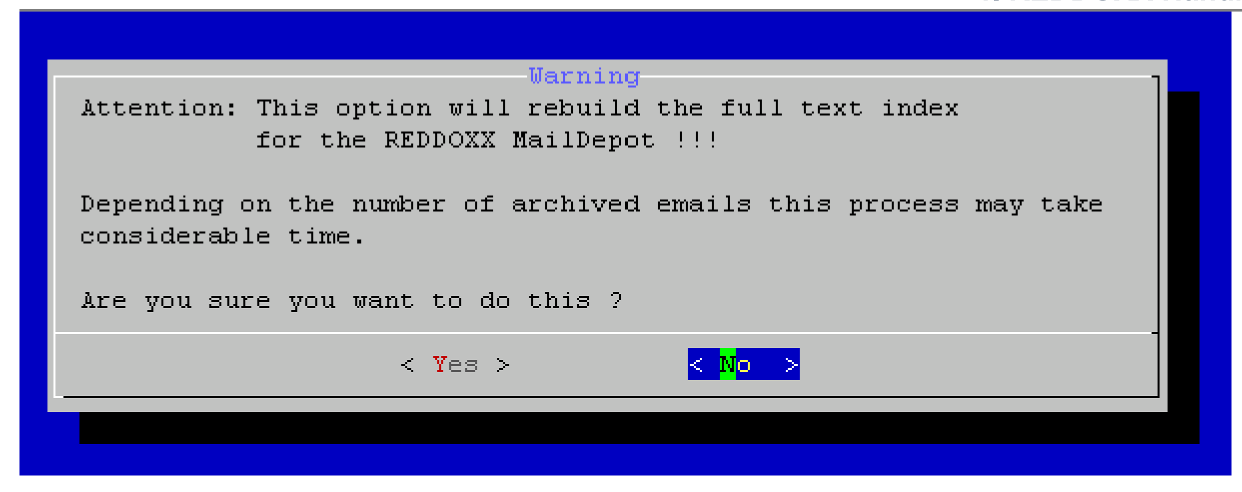
```
Database maintenance
Stopping engine ...
Backup database ...
Restore database ...
Activate new database ...
Starting engine ...

Database reoganisation finished.

Database reoganisation finished.

< EXIT >
```

## 6.3.2 Rebuild the full text index of the MailDepot




Wählen Sie YES, um die komplette Neu-Indizierung Ihres gesamten Archivs zu starten. Folgendes Fenster erscheint:

```
Deleting old index.
Deleting old temp directory.
Waiting for next message in maildepot ...
```

An dieser Stelle wartet der Fulltext-Indexer auf die nächste im Archiv eingehende E-Mail. Dies ist erforderlich, um den exakten Zeitpunkt zu markieren, bis zu dem der Indexer indizieren soll und von wann ab der täglich laufende inkrementelle Indexer starten soll.

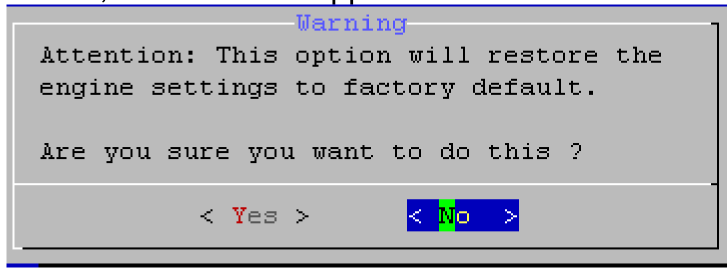
Achten Sie dabei darauf, dass in der Adminkonsole die Option „Volltextindizierung aktivieren“ eingeschaltet ist, sonst wartet der Indexer an dieser Stelle ewig. Falls die Option noch nicht aktiviert war, reicht es aus, sie jetzt zu aktivieren. Der Indexer prüft die Veränderung regelmäßig ab.

Nach Eingang der nächsten Archiv-Mail startet der Indexer und berechnet die Anzahl zu indizierende Mails und schätzt die verbleibende Zeit. An Ende kehrt der Indexer wieder ins Menü zurück.

Der Fulltext-Indexer braucht für ca. 500.000 E-Mails auf einer RX-750 Appliance ca. 24 Stunden.
Es empfiehlt sich, den Indexlauf über das Wochenende zu starten.

### 6.3.3 Set Appliance Settings to Factory Defaults

Hiermit setzen Sie die Netzwerkkonfiguration zum Ursprungszustand zurück. Sie werden vor dem Zurücksetzen nochmals gefragt, ob Sie dies wirklich tun wollen. Brechen Sie mit ***NO*** ab, wenn Sie die Appliance doch nicht zurücksetzen wollen.



### 6.3.4 Re-Create Database

Hiermit werden alle E-Mails, Filterlisten und Benutzerdaten gelöscht. Sie werden vor dem Zurücksetzen nochmals gefragt, ob Sie dies wirklich tun wollen. Brechen Sie mit ***NO*** ab, wenn Sie die Datenbank doch nicht zurücksetzen wollen.

```
Warning
Attention: This option will delete all mails, filter lists and any user
data from the appliance !!!

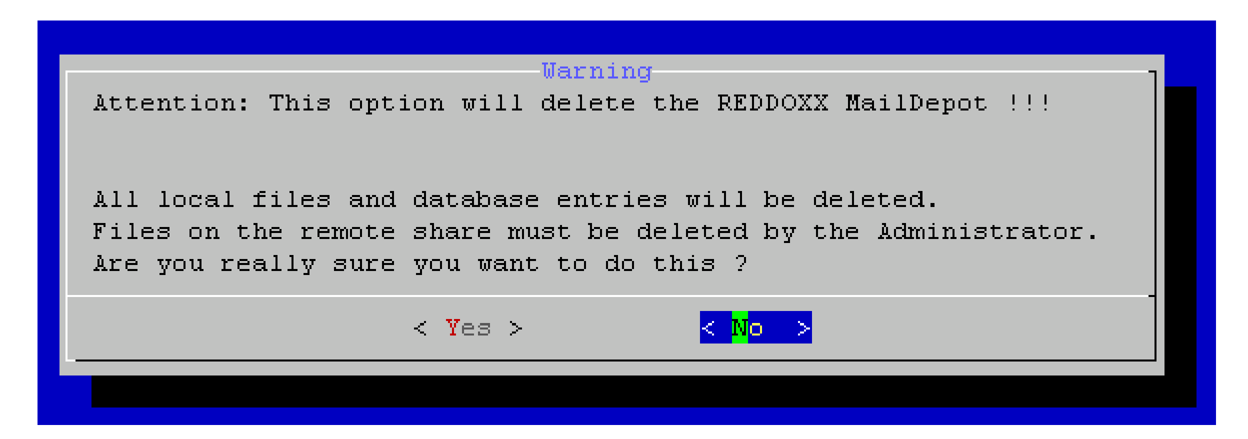
!!! WARNING: ALL DATA WILL BE LOST !!! WARNING: ALL DATA WILL BE LOST !!!

Are you really sure you want to do this ?

< Yes >          < No  >
```

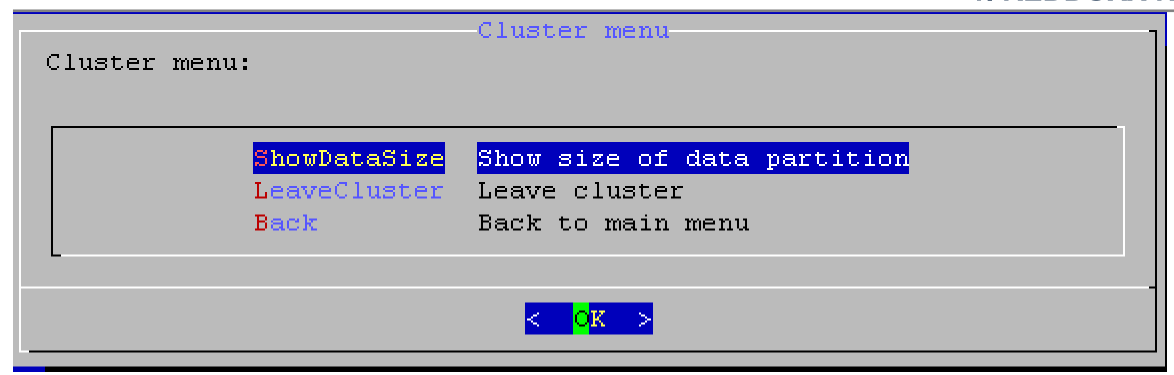
### 6.3.5 Clear MailDepot

Hiermit können Sie alle Mails im MailDepot löschen. Dabei wird die interne Datenbank bereinigt und auch die lokalen Dateien werden auf der Festplatte gelöscht. Archivdateien auf einem Remote-Share muss der Administrator jedoch selbst manuell löschen.

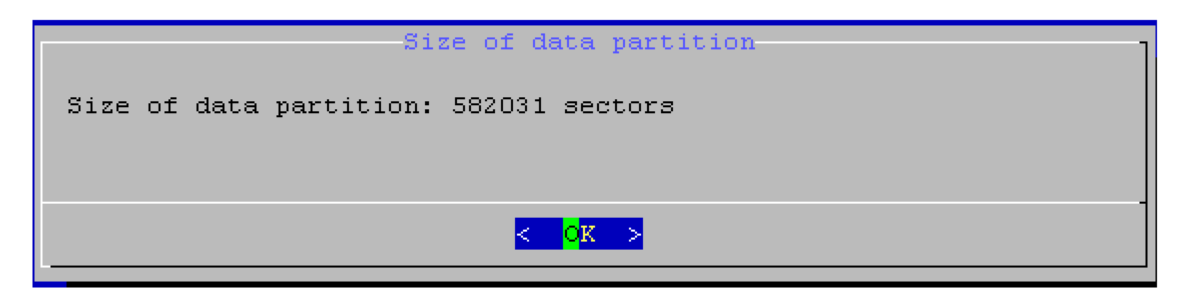



## 6.4 Cluster Options

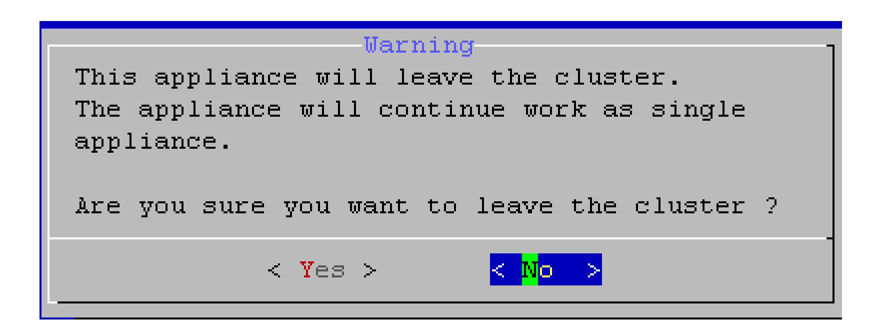
### 6.4.1 Show size of data partition




Überprüfen Sie die Größe der Datenpartition. Vergleichen Sie diesen Wert mit dem der anderen Appliance, mit der Sie den Cluster bilden wollen. Beim Cluster Einrichten darf die Größe der Datenpartition des sekundären Clusterknotens nicht größer sein, als die des primären Knotens.

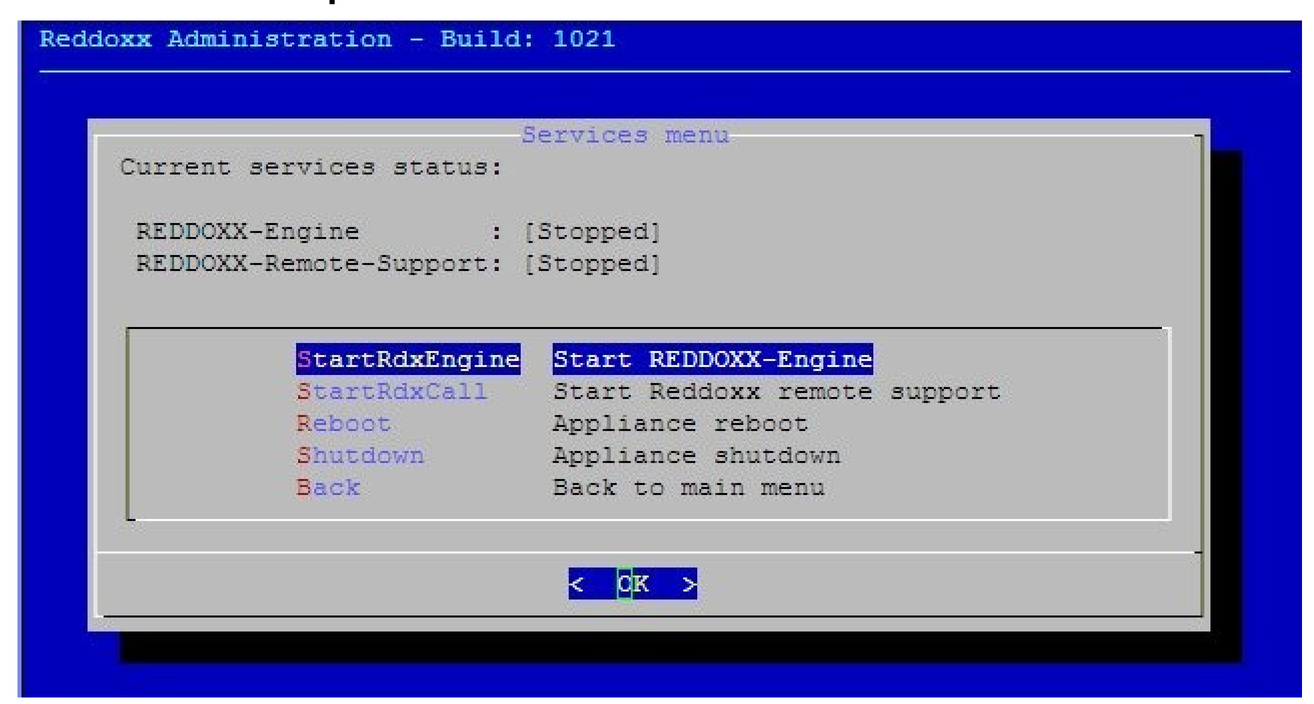



### 6.4.2 Leave Cluster




Wählen Sie „Yes“ wenn Sie den Cluster auflösen möchten. Der Clusterknoten arbeitet danach nach einem Reboot als Single Appliance weiter.

## 6.5 Start and Stop Services




### 6.5.1 Start REDDOXX Engine

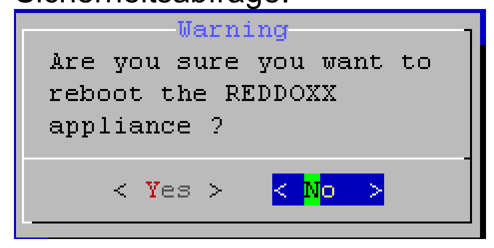
Hiermit können Sie die REDDOXX Engine stoppen und wieder starten.

### 6.5.2 Start REDDOXX Remote Support

Mit dem Starten des Remote Support Services ermöglichen Sie dem Support-Mitarbeiter von REDDOXX den Zugang zu Ihrer REDDOXX Appliance.
Beenden Sie in Absprache mit dem REDDOXX-Support diesen Service.

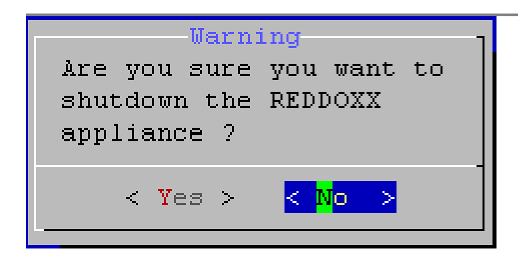
### 6.5.3 Appliance Reboot

Hiermit können Sie die Appliance neu starten. Es erscheint zuvor noch eine Sicherheitsabfrage.




### 6.5.4 Appliance Shutdown

Hiermit können Sie die Appliance ausschalten. Es erscheint zuvor noch eine Sicherheitsabfrage.




## 6.6 Change Admin Password

Hier können Sie das Passwort für den Benutzer *admin* für den Zugang zur Appliance-Konsole ändern. Falls Sie den Dialog abbrechen möchten, drücken Sie CTRL-C.

```
Changing password for admin
Enter the new password (minimum of 5, maximum of 127 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
```

# 7 FAQ - Die häufigsten Fragen

Die häufigsten Fragen über die REDDOXX Appliance und die Antworten.

**HINWEIS**

Eine komplette Liste aller FAQ-Artikel finden Sie im REDDOXX Support Center unter
**http://support.reddoxx.net**

**Frage:**
Was tun bei einem Hardwareausfall?
**Antwort:**
Sofern Sie die Option Next Business Day (NBD) - 24 Stunden Reaktionszeit - gekauft haben, wenden Sie sich bitte direkt an den technischen Support unter:

e-mail: support@reddoxx.net
Wichtig! - Ohne die NBD-Option wenden Sie sich bitte an Ihren Fachhändler.

**Frage:**
Welche Regeln gelten bei den Subject- White- und Blacklisten (SBL / SWL) und nach welchen Kriterien wird gefiltert?
**Antwort:**
1. Es gilt die Teilstringsuche. Der gesamte Ausdruck muss im Betreff vorkommen. Dies gilt auch bei mehreren Wörtern. Ein Leerzeichen gibt genauso wie jedes andere Zeichen.
2. Groß- und Kleinschreibung ist nicht relevant, wird also nicht unterschieden.
3. Es gibt keine Platzhalter oder reguläre Ausdrücke.
4. Umlaute und Sonderzeichen werden derzeit noch nicht berücksichtigt.

**Frage:**
Wie kann der Admin auf E-Mails von Mitarbeitern zugreifen?
**Antwort:**
Für den Fall, dass eine Kontrolle der E-Mails nötig ist, oder eine wichtige E-Mail erwartet wird und der Mitarbeiter im Urlaub ist, kann der Zugriff auf dessen Konto eingerichtet werden. Hierfür muss der Mitarbeiter aber zuvor einen Stellvertreter benannt haben (z.B. den Administrator, oder Vorgesetzten).

**Frage:**
Warum erscheint ein neu angelegter Benutzer im Active Directory nicht in der Spamfinder Benutzerverwaltung?
**Antwort:**
Der Spamfinder greift nur bei aktivierter Empfängerprüfung auf das Active Directory zu. Überprüfen Sie diese Einstellung unter ==> Appliance Konfiguration - SMTP Einstellungen – Lokale Internetdomäne - Reiter LDAP - Empfängerprüfung
Der Benutzer wird im Spamfinder erst angelegt, wenn der Benutzer
- sich an der User-Konsole erstmals anmeldet oder
- erstmals eine E-Mail über den Spamfinder bekommt oder versendet
Darüber hinaus kann es auch sein, dass die Replizierung der Domain Controller noch nicht abgeschlossen ist.
Überprüfen Sie das Protokoll auf etwaige Fehlermeldungen.

**Frage:**
Was kann ich tun, wenn der Bayes Filter nicht funktioniert? Im Protokoll steht RC 3.

**Antwort:**
RC 3 bedeutet: genereller IO-Fehler an der internen Datenbank. Dies tritt äußerst selten auf. Verursacht werden kann das durch Abstürze wie z.B. bei einem Stromausfall. In der Regel kann die interne Datenbank jedoch solche Ausfälle abfangen.
Durch das Löschen der Bayes-Datenbank über die Adminkonsole (in den Filtereinstellungen) wird das Problem behoben.

**Frage:**
Scannt der Virenscanner auch ZIP-Archive?
**Antwort:**
Ja. Zip-Archive werden selbstverständlich von der Viren-Engine gescannt. Ist das Archiv allerdings verschlüsselt bzw. mit einem Passwort belegt, kann ein Virenscanner das Archiv nicht scannen. Sie können dies beispielsweise mit dem Test-Virus namens EICAR testen.

# 8 Anhang

## 8.1 Kontakt und Support

# Kontakt

Wenn Sie Fragen, Anregungen, Lob oder Kritik zur REDDOXX Appliance haben, freuen wir uns auf Ihre E-Mail oder Ihren Anruf.

**REDDOXX GmbH**

Saline 29
D-78628 Rottweil
Fon: +49 (0)741 248 810
Fax: +49 (0)741 248 811
E-Mail: info@REDDOXX.com
Internet: www.REDDOXX.com

# Support

Das Support-Team von REDDOXX setzt alles daran, Kundenbedürfnisse zu befriedigen und Kundenzufriedenheit zu gewährleisten. Daher werden für alle REDDOXX Appliances umfassende Supportmöglichkeiten angeboten, welche unseren Kunden in einem Portal zur Verfügung stehen.
Besuchen Sie hierzu diese Internetseite: http://support.redddoxx.net

## 8.2 Deinstallation und Entsorgung

**REDDOXX Konsolen deinstallieren**

Folgende Schritte beschreiben das Deinstallieren der Administrator-Konsole sowie der Benutzer-Konsole.

**Voraussetzungen:** Die REDDOXX Appliance wird nicht mehr benötigt.

1. Löschen Sie die *rdxadmin.exe* und die *rdxuser.exe* von Ihrem Computer.
2. Setzen Sie Ihr E-Mail-Routing zurück.
3. Trennen Sie die REDDOXX Appliance von allen Anschlüssen.

**REDDOXX Appliance entsorgen**

Entsorgen Sie die Appliance und die zugehörigen Komponenten in Übereinstimmung mit allen nationalen Gesetzen und Bestimmungen.
EAR-Nr.: DE 86380757

## 8.3 Lizenzvereinbarungen

**Allgemeine Geschäftsbedingungen der REDDOXX GmbH, Rottweil, für das Produkt REDDOXX**

1. **Allgemeiner Teil**
1. **Geltungsbereich**

1. Die Allgemeinen Geschäftsbedingungen der REDDOXX GmbH, Saline 29, 78628 Rottweil (im folgenden „REDDOXX“ genannt) für das Produkt Spamfinder (im Folgenden „Spamfinder“ genannt) gelten ausschließlich. Entgegenstehende oder von diesen Allgemeinen Geschäftsbedingungen abweichende Bedingungen des Vertragspartners von REDDOXX (im Folgenden „Besteller“ genannt) werden nicht anerkannt, es sei denn, REDDOXX hat ausdrücklich und schriftlich der Geltung abweichender Bedingungen zugestimmt. Diese Allgemeinen Geschäftsbedingungen gelten auch dann, wenn REDDOXX in Kenntnis entgegenstehender oder von den eigenen Geschäftsbedingungen abweichender Bedingungen des Bestellers die Lieferung an den Besteller vorbehaltlos durchführt.
2. Die Allgemeinen Geschäftsbedingungen gelten auch für alle zukünftigen Geschäfte mit dem Besteller.
3. Die Allgemeinen Geschäftsbedingungen gelten nur gegenüber Unternehmern.

**2. Schutzrechte**

1. An Software und Hardware sowie allen Abbildungen, Zeichnungen, Kalkulationen und sonstigen Unterlagen behält sich REDDOXX das Eigentums- und Urheberrecht vor.
2. Erfolgen Lieferungen nach Zeichnungen oder sonstigen Angaben des Bestellers und werden hierdurch Schutzrechte Dritter geltend gemacht, stellt der Besteller REDDOXX im Innenverhältnis von sämtlichen Ansprüchen frei.

**3. Aufrechnung und Zurückbehaltungsrecht**

1. Das Recht zur Aufrechnung steht dem Besteller nur zu, wenn und soweit seine Gegenansprüche rechtskräftig festgestellt, unbestritten oder von REDDOXX schriftlich anerkannt sind. Das Zurückbehaltungsrecht des Bestellers ist auf Ansprüche aus dem Vertragsverhältnis beschränkt.
2. Wegen Mängeln kann der Besteller Zahlungen nur zu einem unter Berücksichtigung des Mangels verhältnismäßigen Teil zurückbehalten und nur wenn der Mangel zweifelsfrei vorliegt.

**4. Eigentumsvorbehalt**

1. REDDOXX behält sich das Eigentum an sämtlichen gelieferten Teilen bis zum Eingang aller Zahlungen aus der Lieferbeziehung, auch der zukünftig entstehenden Verbindlichkeiten, vor. Bei vertragswidrigem Verhalten, insbesondere bei Zahlungsverzug, ist REDDOXX berechtigt, die Kaufsache zurückzunehmen.
2. Der Besteller ist verpflichtet, die gelieferten Teile pfleglich zu behandeln und während der Dauer des Eigentumsvorbehaltes auf eigene Kosten gegen jede Form des Untergangs zum Neuwert zu versichern. REDDOXX bleibt berechtigt, die Ware auf Kosten des Bestellers selbst zu versichern.
3. Kosten für Wartungs- und Inspektionsarbeiten sind auch während des Eigentumsvorbehaltes von dem Besteller zu tragen, auch, wenn diese von REDDOXX durchgeführt werden.
4. Bei Pfändungen oder sonstigen Eingriffen Dritter hat der Besteller REDDOXX unverzüglich schriftlich zu benachrichtigen, damit diese Drittwiderspruchsklage erheben kann. Soweit der Dritte nicht in der Lage ist, die gerichtlichen und außergerichtlichen Kosten einer solchen Klage zu erstatten, haftet hierfür der Besteller.

**5. Versand, Gefahrübergang**

1. Der Versand erfolgt auf Gefahr des Bestellers. Die Gefahr geht stets, auch wenn weitere Leistungen von REDDOXX übernommen werden, spätestens mit Absendung der Ware auf den Besteller über.
2. Verzögert sich der Versand infolge von Umständen, die REDDOXX nicht zu vertreten hat, so geht die Gefahr vom Tage der Versandbereitschaft auf den Abnehmer über. Auf schriftlichen Wunsch des Bestellers wird die Sendung von REDDOXX gegen Bruch-, Transport-, Feuer- und Wasserschäden auf Kosten des Bestellers versichert.
3. Transport- und alle sonstigen Verpackungen nach Maßgabe der Verpackungsverordnung werden nicht zurückgenommen. Der Besteller ist verpflichtet, die Entsorgung der Verpackung auf eigene Kosten zu besorgen.

**6. Störungen bei der Leistungserbringung**

1. Wenn eine Ursache, die REDDOXX nicht zu vertreten hat, einschließlich Streik oder Aussperrung, die Termineinhaltung beeinträchtigt („Störung“), verschieben sich die Termine um die Dauer der Störung, erforderlichenfalls einschließlich einer angemessenen Wiederanlaufphase. Ein Vertragspartner hat den anderen Vertragspartner über die Ursache einer in seinem Bereich aufgetretenen Störung und die Dauer der Verschiebung unverzüglich zu unterrichten.
2. Erhöht sich der Aufwand aufgrund einer Störung, kann REDDOXX auch die Vergütung des Mehraufwands verlangen, außer der Besteller hat die Störung nicht zu vertreten und deren Ursache liegt außerhalb seines Verantwortungsbereichs.
3. Wenn der Besteller wegen nicht ordnungsgemäßer Leistung von REDDOXX vom Vertrag zurücktreten und/oder Schadensersatz statt der Leistung verlangen kann oder solches behauptet, wird der Besteller auf Verlangen von REDDOXX innerhalb angemessener gesetzter Frist schriftlich erklären, ob er diese Rechte geltend macht oder weiterhin die Leistungserbringung wünscht. Bei einem Rücktritt hat der Besteller REDDOXX den Wert zuvor bestehender Nutzungsmöglichkeiten zu erstatten; gleiches gilt für Verschlechterungen durch bestimmungsgemäßen Gebrauch.

**7. Allgemeine Haftung von REDDOXX**

1. REDDOXX haftet dem Besteller stets:
1. für die von ihr sowie ihren gesetzlichen Vertretern oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursachten Schäden,
2. nach dem Produkthaftungsgesetz und
3. für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die REDDOXX, ihre gesetzlichen Vertreter oder Erfüllungsgehilfen zu vertreten haben.
2. REDDOXX haftet bei leichter Fahrlässigkeit nicht, außer soweit sie eine wesentliche Vertragspflicht (Kardinalpflicht) verletzt hat. Diese Haftung ist bei Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden beschränkt. Dies gilt auch für entgangenen Gewinn und ausgebliebene Einsparungen. Die Haftung für sonstige entferntere Mangelfolgeschäden ist ausgeschlossen. Für einen einzelnen Schadensfall ist die Haftung auf den Vertragswert begrenzt, bei laufender Vergütung auf die Höhe der Vergütung pro Vertragsjahr, jedoch nicht auf weniger als € 50.000. Die Haftung gemäß I 7.1 bleibt von diesem Absatz unberührt.
3. Aus einer Garantieerklärung haftet REDDOXX nur auf Schadensersatz, wenn dies in der Garantie ausdrücklich übernommen wurde. Diese Haftung unterliegt bei leichter Fahrlässigkeit den Beschränkungen gemäß I 7.2.
4. Bei Verlust von Daten haftet REDDOXX nur für denjenigen Aufwand, der für die Wiederherstellung der Daten bei ordnungsgemäßer Datensicherung durch den Besteller erforderlich ist. Bei leichter Fahrlässigkeit von REDDOXX tritt diese

Haftung nur ein, wenn der Besteller unmittelbar vor der zum Datenverlust führenden Maßnahme eine ordnungsgemäße Datensicherung durchgeführt hat.

5. Für Aufwendungsersatzansprüche und sonstige Haftungsansprüche des Bestellers gegen REDDOXX gilt I 7.1 bis 7.4 entsprechend.

**8. Geheimhaltung**

1. Die Parteien verpflichten sich wechselseitig, gegenüber Dritten über alle ihnen im Rahmen der Zusammenarbeit zur Kenntnis gelangenden geschäftlichen Vorgänge, insbesondere über Geschäfts- und Betriebsgeheimnisse, absolutes Stillschweigen zu bewahren. Die Geheimhaltungsverpflichtung besteht auch nach Beendigung des Vertrages fort.
2. Sämtliche wechselseitig ausgetauschten Geschäftsunterlagen sind sorgfältig in den eigenen Geschäftsräumen zu verwahren und vor Einsichtnahme Unbefugter zu schützen.

**9. Abtretungsverbot**

1. Sämtliche Ansprüche des Bestellers aus dem Vertragsverhältnis gegen REDDOXX sind nicht abtretbar.

**10. Produkthaftung**

1. Der Besteller darf den Spamfinder nur bestimmungsgemäß verwenden und muss dafür sorgen, dass der Spamfinder nur an mit den Produktgefahren und -risiken vertraute Personen weiterveräußert wird.
2. Der Besteller ist verpflichtet, bei Verwendung des Spamfinders als Grundstoff und Teilprodukt von eigenen Produkten beim Inverkehrbringen des Endprodukts seiner Warnpflicht auch im Hinblick auf die von REDDOXX gelieferte Ware nachzukommen. Im Innenverhältnis stellt der Besteller REDDOXX von der Geltendmachung von Ansprüchen bei Verletzung dieser Obliegenheit auf erstes Anfordern frei.

**11. Erfüllungsort, Gerichtsstand, Rechtswahl, USA-Rechtsvorschriften**

1. Erfüllungsort ist Rottweil.
2. Gerichtsstand für sämtliche Streitigkeiten aus dem Vertrag ist Rottweil. REDDOXX ist jedoch berechtigt, den Besteller auch an seinem allgemeinen Gerichtsstand oder an dem Sitz einer Niederlassung des Bestellers zu verklagen.
3. Es gilt ausschließlich deutsches Recht unter Ausschluss des UN-Kaufrechts.
4. Der Besteller wird für die Lieferungen oder Leistungen anzuwendende Import- und Export-Vorschriften eigenverantwortlich beachten, insbesondere solche der USA. Bei grenzüberschreitender Lieferung oder Leistung trägt der Besteller anfallende Zölle, Gebühren und sonstige Abgaben. Der Besteller wird gesetzliche oder behördliche Verfahren im Zusammenhang mit grenzüberschreitenden Lieferungen oder Leistungen eigenverantwortlich abwickeln, außer soweit anderes ausdrücklich vereinbart ist.

**2. Regelungen für den Kauf des Spamfinders**

**I. Vertragsgegenstand**

I. Die Beschaffenheit und der Leistungsumfang des Spamfinders sowie die freigegebene Einsatzumgebung ergeben sich aus der Produktbeschreibung.

II. Der Spamfinder wird einschließlich einer Bedienungsanleitung (Benutzungsdokumentation oder Online-Hilfe) und der Installationsanleitung geliefert. Die Bedienungsanleitung und die Installationsanleitung können dem Besteller auch elektronisch zur Verfügung gestellt werden.

III. Der Spamfinder wird vom Besteller installiert.

**II. Einsatzrechte am Spamfinder und Schutz vor unberechtigter Nutzung**

I. REDDOXX räumt dem Besteller mit vollständiger Bezahlung der geschuldeten Vergütung das Recht ein, den Spamfinder in dem im Vertrag festgelegten Umfang einzusetzen. Ist der Umfang im Vertrag nicht vereinbart, ist dies ein einfaches, nicht ausschließliches Nutzungsrecht zum Einsatz auf Dauer. Dies berechtigt den Besteller nur zum Einsatz des Spamfinders an einem Computer durch einen einzelnen Nutzer zur gleichen Zeit. Das Nutzungsrecht umfasst nur den Einsatz für interne Zwecke des Bestellers. Eine erweiterte Nutzung ist stets vor ihrem Beginn vertraglich zu vereinbaren. Die Vergütung richtet sich nach dem Umfang des Einsatzrechts.

II. Der Besteller darf die Software des Spamfinders nur kopieren, soweit dies für den vertragsgemäßen Einsatz erforderlich ist. Urheberrechtsvermerke in der Software dürfen nicht verändert oder gelöscht werden.

III. REDDOXX ist berechtigt, angemessene technische Maßnahmen zum Schutz vor einer nicht vertragsgemäßen Nutzung zu treffen. Der Einsatz des Spamfinders auf einer Ausweich- oder Nachfolgekonfiguration darf dadurch nicht wesentlich beeinträchtigt werden.

IV. Das Eigentum an überlassenen Vervielfältigungsstücken bleibt vorbehalten bis zur vollständigen Bezahlung der geschuldeten Vergütung. Zuvor sind Einsatzrechte stets nur vorläufig und durch REDDOXX frei widerruflich eingeräumt.

V. REDDOXX kann das Einsatzrecht des Bestellers widerrufen, wenn dieser nicht unerheblich gegen Einsatzbeschränkungen oder sonstige Regelungen zum Schutz vor unberechtigter Nutzung verstößt. REDDOXX hat dem Besteller vorher eine Nachfrist zur Abhilfe zu setzen. Im Wiederholungsfall und bei besonderen Umständen, die unter Abwägung der beiderseitigen Interessen den sofortigen Widerruf rechtfertigen, kann REDDOXX den Widerruf ohne Fristsetzung aussprechen. Der Besteller hat REDDOXX die Einstellung der Nutzung nach dem Widerruf schriftlich zu bestätigen.

**III. Pflichten des Bestellers**

I. Der Besteller benennt einen verantwortlichen Ansprechpartner. Dieser kann und wird für den Besteller verbindliche Entscheidungen treffen oder unverzüglich herbeiführen. Der Ansprechpartner steht REDDOXX für notwendige Informationen zur Verfügung.

II. Der Besteller sorgt dafür, dass spätestens im Zeitpunkt der Lieferung fachkundiges Personal für den Einsatz des Spamfinders zur Verfügung steht.

III. Der Besteller wird REDDOXX unverzüglich über Änderungen des Einsatzumfeldes unterrichten.

IV. Der Besteller hat Mängel in nachvollziehbarer und detaillierter Form unter Angabe aller für die Mängelerkennung und -analyse zweckdienlichen Informationen schriftlich zu melden. Anzugeben sind dabei insbesondere die Arbeitsschritte, die zum Auftreten des Mangels geführt haben, die Erscheinungsform sowie die Auswirkungen des Mangels.

V. Der Besteller hat REDDOXX soweit erforderlich bei der Beseitigung von Mängeln zu unterstützen, insbesondere auf Wunsch von REDDOXX Arbeitsmittel zur Verfügung zu stellen.

VI. Der Besteller erkennt an, dass der Spamfinder samt der Bedienungsanleitung und weiterer Unterlagen - auch in künftigen Versionen - urheberrechtlich geschützt sind. Insbesondere Quellprogramme sind Betriebsgeheimnisse von REDDOXX. Der Besteller trifft zeitlich unbegrenzte Vorsorge, dass Quellprogramme ohne Zustimmung von REDDOXX Dritten nicht zugänglich werden.

VII. Der Besteller darf nichts unternehmen, was einer unberechtigten Nutzung Vorschub leisten könnte. Insbesondere darf er nicht versuchen, die Programme zu dekompilieren. Der Besteller wird REDDOXX unverzüglich unterrichten, wenn er Kenntnis davon hat, dass in seinem Bereich ein unberechtigter Zugriff droht oder erfolgt ist.

**IV. Mangelansprüche des Bestellers**

I. Für eine nur unerhebliche Abweichung der Leistungen von REDDOXX von der vertragsgemäßen Beschaffenheit oder Brauchbarkeit bestehen keine Ansprüche wegen Sachmängeln. Ansprüche wegen Mängeln bestehen auch nicht bei übermäßiger oder unsachgemäßer Nutzung, natürlichem Verschleiß, Versagen von Komponenten der Systemumgebung, nicht reproduzierbaren oder anderweitig durch den Besteller nachweisbaren Softwarefehlern oder bei Schäden, die aufgrund besonderer äußerer Einflüsse entstehen, die nach dem Vertrag nicht vorausgesetzt sind. Dies gilt auch bei nachträglicher Veränderung oder Instandsetzung durch den Besteller oder Dritte, außer diese erschwert die Analyse und die Beseitigung eines Sachmangels nicht. Für Schadensersatz- und Aufwendungsersatzansprüche gilt I 7 ergänzend.

II. Ansprüche wegen eines Sachmangels verjähren innerhalb eines Jahres ab dem gesetzlichen Verjährungsbeginn. Die gesetzlichen Fristen für den Rückgriffsanspruch nach § 478 BGB bleiben unberührt, gleiches gilt bei einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Bestellers, bei arglistigem Verschweigen eines Mangels sowie in den Fällen der Verletzung des Lebens, des Körpers oder der Gesundheit.

III. Die Bearbeitung einer Sachmangelanzeige des Bestellers durch REDDOXX führt nur zur Hemmung der Verjährung, soweit die gesetzlichen Voraussetzungen dafür vorliegen. Ein Neubeginn der Verjährung tritt dadurch nicht ein.

IV. Eine Nacherfüllung (Neulieferung oder Nachbesserung) kann ausschließlich auf die Verjährung des die Nacherfüllung auslösenden Mangels Einfluss haben.

V. Der Besteller hat Mangelansprüche nur, wenn gemeldete Mängel reproduzierbar oder anderweitig durch den Besteller nachweisbar sind. Für die Mitteilung von Mängeln gilt insbesondere II 3.4.

VI. Stehen dem Besteller Mangelansprüche zu, hat er zunächst nur das Recht auf Nacherfüllung innerhalb einer angemessen Frist. Die Nacherfüllung beinhaltet nach Wahl von REDDOXX entweder Nachbesserung oder die Lieferung einer Ersatzsoftware. Die Interessen des Bestellers werden bei einer Wahl angemessen berücksichtigt.

VII. Schlägt die Nacherfüllung fehl oder ist sie aus anderen Gründen nicht durchzuführen, kann der Besteller unter den gesetzlichen Voraussetzungen die Vergütung mindern, vom Vertrag zurücktreten und/oder Schadens- oder Aufwendungsersatz verlangen. Der Besteller übt ein ihm zustehendes Wahlrecht für Mangelansprüche innerhalb einer angemessenen Frist aus, in der Regel innerhalb von 14 Kalendertagen.

VIII. REDDOXX kann Vergütung ihres Aufwands verlangen, soweit

I. sie aufgrund einer Meldung tätig wird, ohne dass ein Mangel vorliegt, außer der Besteller konnte mit zumutbarem Aufwand nicht erkennen, dass kein Mangel vorlag, oder

II. eine gemeldete Störung nicht reproduzierbar oder anderweitig durch den Besteller als Mangel nachweisbar ist, oder

III. zusätzlicher Aufwand wegen nicht ordnungsgemäßer Erfüllung der Pflichten des Bestellers (siehe auch II 3) anfällt.

**V. Rechtsmängel**

I. Für Verletzungen von Rechten Dritter durch seine Leistung haftet REDDOXX nur, soweit die Leistung vertragsgemäß und insbesondere im vertraglich vorgesehenen Nutzungsumfeld eingesetzt wird.

II. REDDOXX haftet für Verletzungen von Rechten Dritter nur innerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes sowie am Ort der vertragsgemäßen Nutzung der Leistung.

III. Macht ein Dritter gegenüber dem Besteller geltend, dass eine Leistung von REDDOXX seine Rechte verletzt, benachrichtigt der Besteller unverzüglich REDDOXX. REDDOXX und ggf. dessen Vorlieferanten sind berechtigt, aber nicht verpflichtet, soweit zulässig die geltend gemachten Ansprüche auf deren Kosten abzuwehren.

IV. Werden durch eine Leistung von REDDOXX Rechte Dritter verletzt, wird REDDOXX nach eigener Wahl und auf eigene Kosten

I. dem Besteller das Recht zur Nutzung der Leistung verschaffen oder

II. die Leistung rechtsverletzungsfrei gestalten oder

III. die Leistung unter Erstattung der dafür vom Besteller geleisteten Vergütung (abzüglich einer angemessenen Nutzungsentschädigung) zurücknehmen, wenn REDDOXX keine andere Abhilfe mit angemessenem Aufwand erzielen kann. Die Interessen des Bestellers werden dabei angemessen berücksichtigt.

**6. Kaufpreiszahlung**

1. Der Kaufpreis ist sofort fällig.
2. REDDOXX räumt dem Besteller eine Zahlungsfrist von 4 Wochen ab Versand des Spamfinders ein.

**7. Fehlfunktionen des Spamfinders**

1. Der Besteller wird ausdrücklich darauf hingewiesen, dass eine von ihm fehlerhaft veranlasste Konfiguration, Klassifizierung und Administrierung des Spamfinders zu Fehlfunktionen führen kann. Die Konfiguration, Klassifizierung und Administrierung liegt allein im Verantwortungsbereich des Bestellers.

**3. Virenschutz**

1. Der Spamfinder nutzt ClamAV-Software als Virenschutz. Bezüglich des Virenschutzmoduls des Spamfinders gelten die Lizenzbestimmungen von ClamAV und können unter www.clamav.org nachgelesen werden. ClamAV steht unter der GPL.

**4. Regelungen für die Softwarepflege des Spamfinders**

**1. Vertragsgegenstand**

1. REDDOXX erbringt die nachfolgend vereinbarten Pflegeleistungen nur für die jeweils aktuelle Version des als Pflegegegenstand vereinbarten Spamfinders gegen die vereinbarte Vergütung.
2. REDDOXX erbringt folgende Pflegeleistungen:

1. Störungsmanagement: REDDOXX wird Störungsmeldungen des Bestellers entgegen nehmen, den vereinbarten Störungskategorien zuordnen und anhand dieser Zuordnung die vereinbarten Maßnahmen zur Analyse und Bereinigung von Störungen durchführen. Das Störungsmanagement umfasst keine Leistungen, die im Zusammenhang mit dem Einsatz des Spamfinders in nicht freigegebenen Umgebungen oder mit Veränderungen des Spamfinders durch den Besteller oder Dritten stehen.
2. Annahme von Störungsmeldungen des Bestellers: REDDOXX wird während ihrer üblichen Geschäftszeiten ordnungsgemäße Störungsmeldungen des Bestellers entgegen nehmen und jeweils mit einer Kennung versehen. Auf Anforderung des Bestellers bestätigt ihm REDDOXX den Eingang einer Störungsmeldung unter Mitteilung der vergebenen Kennung.
3. Durchführung von Maßnahmen zur Störungsbeseitigung: Bei Meldungen über schwerwiegende Störungen und sonstige Störungen wird REDDOXX kurzfristig anhand der vom Besteller mitgeteilten Umstände entsprechende Maßnahmen einleiten, um zunächst die Störungsursache zu lokalisieren. Stellt sich die mitgeteilte Störung nach erster Analyse nicht als Fehler des Spamfinders dar, teilt REDDOXX dies dem Besteller unverzüglich mit. Sonst wird REDDOXX entsprechende Maßnahmen zur weitergehenden Analyse und zur Bereinigung der mitgeteilten Störung veranlassen. REDDOXX wird dem Besteller bei ihm vorliegenden Maßnahmen zur Umgehung oder Bereinigung eines Fehlers des Spamfinders, etwa Handlungsanweisungen oder Korrekturen des Spamfinders, unverzüglich zur Verfügung stellen. Der Besteller wird solche Maßnahmen zur Umgehung oder Bereinigung von Störungen unverzüglich übernehmen und REDDOXX bei deren Einsatz etwa verbleibende Störungen unverzüglich erneut melden.
4. Überlassung neuer Versionen: REDDOXX stellt dem Besteller die Neuen Versionen des Spamfinders zur Verfügung, um diese auf dem aktuellen Stand zu halten und Störungen vorzubeugen. Die Neuen Versionen werden auf die Box des Bestellers aufgespielt und von dort durch den Besteller selbst installiert.
5. REDDOXX überlässt dem Besteller dazu Updates des Spamfinders mit technischen Modifikationen und Verbesserungen sowie kleineren funktionalen Erweiterungen und Verbesserungen. Weiterhin überlässt REDDOXX dem Besteller dazu Patches mit Korrekturen zum Spamfinder und sonstige Umgehungsmaßnahmen für mögliche Störungen. Diese neuen Stände des Spamfinders werden zusammen als „Neue Versionen“ bezeichnet. Nicht Gegenstand der Pflegeleistungen ist die Überlassung von Upgrades mit wesentlichen funktionalen Erweiterungen oder von neuen Produkten oder Verpflichtungen zur Weiterentwicklung des Spamfinders, außer anderes ist ausdrücklich vereinbart.
6. Der Besteller wird Neue Versionen unverzüglich untersuchen und erkennbare Mängel unverzüglich rügen, wofür § 377 HGB entsprechend gilt. Soweit REDDOXX dem Besteller eine Neue Version zur Verfügung gestellt hat, pflegt er auch die Vorversion noch für eine angemessene Übergangsfrist, die in der Regel drei Monate nicht überschreitet, weiter. Wegen der Neuen Versionen hat der Besteller Mangelansprüche nur, wenn gemeldete Mängel reproduzierbar oder anderweitig durch den Besteller nachweisbar sind.
7. Ansprechstelle (Hotline):REDDOXX richtet eine Ansprechstelle für den Besteller ein (Hotline). Diese Stelle bearbeitet die Anfragen des Bestellers im Zusammenhang mit den technischen Einsatzvoraussetzungen und -bedingungen des Spamfinders sowie einzelnen funktionalen Aspekten. Von der Hotline werden keine Leistungen erbracht, die im Zusammenhang mit dem Einsatz des Spamfinders in nicht freigegebenen Umgebungen oder mit Veränderungen des Spamfinders durch den Besteller oder Dritten stehen. Die Hotline steht montags bis Freitags von 08.00 Uhr bis 17.00 Uhr außerhalb der gesetzlichen Feiertage zur Befragung zur Verfügung. Für die Einordnung der gesetzlichen Feiertage ist der Firmensitz von REDDOXX ausschlaggebend. Der Besteller benennt gegenüber REDDOXX nur fachlich und technisch entsprechend qualifiziertes Personal, das intern beim Besteller mit der Bearbeitung von Anfragen der Anwender des Spamfinders betraut ist. Nur dieses REDDOXX benannte Personal wird Anfragen an die Hotline richten und dabei von REDDOXX gestellte Formulare verwenden. Die Hotline nimmt solche Anfragen per E-Mail, Telefax und Telefon während der üblichen Geschäftszeiten von REDDOXX entgegen. Die Hotline wird ordnungsgemäße Anfragen im üblichen Geschäftsgang bearbeiten und soweit möglich beantworten. Die Hotline kann zur Beantwortung auf dem Besteller vorliegende Dokumentationen und sonstige Ausbildungsmittel für den Spamfinder verweisen. Soweit eine Beantwortung durch die Hotline nicht oder nicht zeitnah möglich ist, wird REDDOXX die Anfrage zur Bearbeitung weiterleiten, insbesondere Anfragen zu nicht von ihm gelieferter Hard- oder Software. Weitergehende Leistungen der Hotline, etwa andere Ansprechzeiten und -fristen sowie Rufbereitschaften oder Einsätze von REDDOXX vor Ort beim Besteller sind vorab ausdrücklich zu vereinbaren.
8. Zusätzliche Leistungen: Über die Ziffern 1.2.1 bis 1.2.5 hinausgehende Leistungen sind nach diesem Vertrag nicht geschuldet, bedürfen gesonderter Vereinbarung und sind gesondert zu vergüten.
9. Austausch des Spamfinders: Bei einem Austausch des Spamfinders ist der Besteller dafür verantwortlich, dass sich keine vertraulichen Informationen im Spamfinder befinden. Auch sorgt der Besteller dafür, dass während des Austausches ein sicherer und ordnungsgemäßer Zugang von elektronischen Nachrichten erfolgt.

**2. Laufzeit**

1. Das Vertragsverhältnis läuft für einen Zeitraum von einem Jahr nach Vertragsschluss.
2. Der Besteller kann einen neuen Vertrag binnen 30 Tagen nach Ende Vertragslaufzeit zu den dann jeweils gültigen Konditionen abschließen.

**3. Nutzungsrecht**

1. Die Nutzungsrechte des Bestellers an Neuen Versionen und an sonstigen Korrekturen des Spamfinders entsprechen den Nutzungsrechten an der vorhergehenden Version des Spamfinders. Hinsichtlich der Nutzungsrechte treten die Rechte an den Neuen Versionen und sonstigen Korrekturen nach einer angemessenen Übergangszeit - die in der Regel nicht mehr als einen Monat beträgt - an die Stelle der Rechte an den vorangegangenen Versionen und sonstigen Korrekturen. Der Besteller darf ein Vervielfältigungsstück archivieren.

**4. Pflichten des Bestellers**

1. Der Besteller benennt einen verantwortlichen Ansprechpartner. Dieser kann für den Besteller verbindliche Entscheidungen treffen oder unverzüglich herbeiführen. Der Ansprechpartner steht REDDOXX für notwendige Informationen zur Verfügung.
2. Der Besteller wird REDDOXX unverzüglich über Änderungen des Einsatzumfeldes unterrichten. Darüber hinaus stellt der Besteller sicher, dass der Spamfinder nur in einer freigegebenen und durch den Spamfinder unterstützten Umgebung eingesetzt wird.
3. Der Besteller hat Störungen in nachvollziehbarer und detaillierter Form unter Angabe aller für die Störungserkennung und -analyse zweckdienlichen Informationen schriftlich zu melden. Anzugeben sind dabei insbesondere die Arbeitsschritte, die zum Auftreten der Störung geführt haben, die Erscheinungsweise sowie die Auswirkungen der Störung.
4. Der Besteller sorgt dafür, dass fachkundiges Personal für die Unterstützung von REDDOXX zur Verfügung steht.

5. Der Besteller ist verpflichtet, REDDOXX soweit erforderlich zu unterstützen und in seiner Betriebssphäre alle zur ordnungsgemäßen Auftragsausführung erforderlichen Voraussetzungen zu schaffen, insbesondere einen Remotezugang auf das Bestellersystem zu ermöglichen und sonstiges Analysematerial zur Verfügung zu stellen. Darüber hinaus stellt der Besteller auf Wunsch von REDDOXX unentgeltlich ausreichende Arbeitsplätze und Arbeitsmittel zur Verfügung.
6. Soweit nichts anderes vereinbart ist, wird der Besteller alle REDDOXX übergebenen Unterlagen, Informationen und Daten bei sich zusätzlich so verwahren, dass diese bei Beschädigung und Verlust von Datenträgern rekonstruiert werden können.
7. Der Besteller gestattet REDDOXX den Zugriff auf die Software mittels Telekommunikation. Die hierfür erforderlichen Verbindungen stellt der Besteller nach Anweisung von REDDOXX her.
8. REDDOXX kann zusätzliche Vergütung seines Aufwands verlangen, soweit:
1. sie aufgrund einer Meldung tätig wird, ohne dass ein Mangel vorliegt, außer der Besteller konnte mit zumutbarem Aufwand nicht erkennen, dass kein Mangel vorlag, oder
2. eine gemeldete Störung nicht reproduzierbar oder anderweitig durch den Besteller als Mangel nachweisbar ist oder
3. zusätzlicher Aufwand wegen nicht ordnungsgemäßer Erfüllung der Pflichten des Bestellers anfällt.

**5. Vergütung**

1. Das Pflegeentgelt wird jährlich berechnet und ist jeweils im Voraus zu entrichten.

**5. Regelungen für die Nutzung von Internetseiten**

**I. Leistungen von REDDOXX**

I. REDDOXX stellt eine Internetseite zur Bestätigung erwünschter Mails zur Verfügung. Über diese Internetseite kann der Besteller unter anderem seinen Spamfinder administrieren.

II. REDDOXX erbringt die unter V 1.1 genannten Leistungen mit einer Gesamtverfügbarkeit von 98 %. Die Verfügbarkeit berechnet sich auf der Grundlage der im Vertragszeitraum auf das jeweilige Kalenderjahr entfallenden Zeit.

**II. Passwort**

I. Für den Zugriff auf die für den Betrieb des Spamfinders notwendigen Internetseiten erhält der Besteller ein veränderbares Passwort. Der Besteller hat mit seinem Passwort die Möglichkeit, den Spamfinder zu konfigurieren und trägt die alleinige Verantwortung für die Konfiguration.

II. Der Besteller ist verpflichtet, das Passwort in regelmäßigen Abständen, mindestens jedoch einmal monatlich zu ändern. Das Passwort muss eine Mindestlänge von 8 Zeichen aufweisen und mindestens einen Buchstaben und eine Ziffer enthalten. Der Besteller darf das Passwort nur an solche Personen weitergeben, die von ihm berechtigt wurden, auf den Speicherplatz Zugriff zu nehmen. Wird das Passwort dreimal in Folge unrichtig eingegeben, so wird der Zugriff auf die für den Betrieb des Spamfinders notwendigen Internetseiten zum Schutz vor Missbräuchen gesperrt. Der Besteller wird hierüber informiert. Er erhält dann von REDDOXX ein neues Passwort zugeteilt.

**III. Zugangssperre**

I. REDDOXX kann eine Zugangssperre verhängen, wenn der Besteller mit Zahlungen in Verzug ist oder den Spamfinder entgegen den vertraglichen Regelungen nutzt. REDDOXX kann darüber hinaus eine Zugangssperre verhängen, wenn der Besteller bei der Nutzung des Spamfinders oder durch die Veröffentlichung auf Internetseiten gegen Gesetze, behördliche Auflagen oder Rechte Dritter verstößt. Dies gilt beispielsweise für die Veröffentlichungen pornografischer oder verfassungsfeindlicher Inhalte. Der Besteller hat REDDOXX von jeglicher Inanspruchnahme durch Dritte einschließlich der durch die Inanspruchnahme ausgelösten Kosten freizustellen.

**IV. Konfiguration**

1. Für die Konfiguration ist der Besteller verantwortlich. Fehlfunktionen, die sich aus einer fehlerhaften oder unvollständigen Konfiguration ergeben, sind nicht von REDDOXX zu vertreten.

**5. Leistungsänderungen**

1. REDDOXX ist berechtigt, die zur Erbringung der Leistungen eingesetzte Hard- und Software an den jeweiligen Stand der Technik anzupassen. Ergeben sich aufgrund einer solchen Anpassung zusätzliche Anforderungen, um das Erbringen der Leistungen von REDDOXX zu gewährleisten, so wird REDDOXX dem Besteller diese zusätzlichen Anforderungen mitteilen. Der Besteller wird unverzüglich nach Zugang der Mitteilung darüber entscheiden, ob die zusätzlichen Anforderungen erfüllt werden sollen und bis wann dies geschehen wird. Erklärt der Besteller nicht bis spätestens vier Wochen vor dem Umstellungszeitpunkt, dass er seine Technik rechtzeitig zur Umstellung, dass heißt spätestens drei Werktage vor dem Umstellungszeitpunkt, an die zusätzlichen Anforderungen anpassen wird, hat REDDOXX das Recht, das Vertragsverhältnis mit Wirkung zum Umstellungszeitpunkt zu kündigen.

**6. Mitwirkungspflichten des Bestellers**

1. Der Besteller wird ferner darauf achten, dass von ihm installierte Programme, Skripte o. ä. den Betrieb des Servers oder des Kommunikationsnetzes von REDDOXX nicht gefährden. Der Besteller stellt REDDOXX von jeglicher von ihm zu vertretenden Inanspruchnahme durch Dritte einschließlich der durch die Inanspruchnahme ausgelösten Kosten frei.
2. Gefährden oder beeinträchtigen vom Besteller installierte Programme, Skripte o. ä. den Betrieb des Servers oder des Kommunikationsnetzes von REDDOXX, so kann REDDOXX diese Programme, Skripte etc. deaktivieren oder deinstallieren. Falls die Beseitigung der Gefährdung oder Beeinträchtigung dies erfordert, ist REDDOXX auch berechtigt, die Anbindung an den Internetseiten zu unterbrechen. REDDOXX wird den Besteller über diese Maßnahme unverzüglich informieren.

# 9 Glossar

## A

**ABL Filter:** Address-Blacklist Filter - Prüfung der Absenderadresse gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. den Benutzer.

**Advanced RBL Filter:** Advanced Realtime Blacklist Filter - Es werden alle E-Mail-Server, die an dem Transport der eingehenden E-Mail mitgewirkt haben, gegen öffentliche Blacklist-Server geprüft. Für die Funktion der ausgewählten Blacklist-Server, sowie die Fehlerfreiheit der Listeinträge auf den Blacklist-Servern wird keine Gewähr übernommen.

**Appliance:** Die Appliance ist die Hardwarekomponente des Spamfinders - die REDDOXX Appliance. Es gibt drei Varianten der REDDOXX Appliance. So ist sichergestellt, dass die Bedürfnisse aller Unternehmensgrößen und E-Mail-Aufkommen optimal abgedeckt werden. Beachten Sie die Warn- und Sicherheitshinweise!

**AWL Filter:** Adressen Whitelist Filter - Autorisierung der Absenderadresse gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Einige Filter bauen diese Liste automatisch auf. Die weitere Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Anwender.

## B

**Bayes Filter:** Der Bayes Filter ermittelt über die inhaltliche Prüfung nach dem bayesischen Verfahren eine Wahrscheinlichkeit, ob es sich um Spam handelt oder nicht. Die Wortlisten werden automatisch durch den Spamfinder aufgebaut. Für eine Falscherkennung wird keine Gewähr übernommen.

## C

**CISS:** Confirmation Interactive Site Server, kurz CISS, ist ein einmaliger, mehrstufiger Kontrollvorgang, der den dauerhaften Austausch von gewollten E-Mails zwischen Sender und Empfänger sicherstellt. Intelligente Autorisierung des Absenders mittels CISS (zum Patent angemeldet), einer einzigartigen Challenge/Response-Funktionalität.

**CISS Filter:** Confirmation Interactive Site Filter - Dieses Verfahren stellt sicher, dass es sich bei dem Absender um eine natürliche Person handelt. Dazu wird über das im Internet erreichbare Spamfinder-Portal eine entsprechende Internetseite zur Verfügung gestellt. Die Verfügbarkeit des Spamfinder-Portals liegt bei mindestens 98,5% pro Jahr.

**Cluster:** Ein Cluster bezeichnet eine Anzahl von vernetzten Computern. Diese vernetzten Computer stehen zur parallelen Abarbeitung zur Verfügung. Abgearbeitet werden Teilaufgaben, die zu einer Aufgabe gehören. Im Gegensatz zu Parallelrechnern findet die Lastverteilung auf der Ebene einzelner Prozesse statt, die auf einer oder verschiedenen Maschinen des Clusters gestartet werden. Man benötigt also keine parallelisierte Software oder spezielle Betriebssysteme, wohl aber einen Scheduler,

der die Teilaufgaben den Einzelrechnern zuweist. Alternativ werden Cluster auch zum Steigern der Verfügbarkeit von Systemen genutzt.

## D

**DBL Filter:** Domänen Blacklist Filter - Prüfung der Absenderdomäne gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

**DMZ:** Bedeutet Demilitarisierte Zone. Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz.
DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

**DNS:** Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Das DNS ist eine verteilte Datenbank, die den Namensraum im Internet verwaltet.

**Domäne:** Eine Domäne (englisch domain) ist ein zusammenhängender Teilbereich des hierarchischen DNS Namensraumes. Eine Domäne umfasst ausgehend vom ihrem Domänennamen immer die gesamte untergeordnete Baumstruktur.

**DWL Filter:** Domänen Whitelist Filter - Autorisierung der Absenderdomäne gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

## F

**Failover:** Failover bezeichnet eine Technologie aus der Informationstechnik, mit deren Hilfe Daten und Dienste hochverfügbar gehalten werden können.

## H

**Hostname:** Der Name der REDDOXX Appliance im Netzwerk.

## K

**Konsole:** Softwarekomponente, über die die REDDOXX Appliance gesteuert wird.

## L

**LDAP:** LDAP (Lightweight Directory Access Protocol) ist ein Netzwerkprotokoll, das bei so genannten Directories zum Einsatz kommt. Es vermittelt die Kommunikation zwischen dem LDAP-Client (beispielsweise einem E-Mail-Server oder digitalen Adressbuch) mit dem Directory Server. Dabei werden alle protokollspezifischen Funktionen geboten, die für eine solche Kommunikation notwendig sind: Anmeldung an dem Server, die Suchabfrage und die Modifikation der Daten.

## M

**Mail Hop:** Mail Hop ist, wenn eine E-Mail von einem Server zu einem anderen Server übermittelt wird, jeder dieser Server wird als Mailhop angesehen.

## N

**NBL Filter:** Netzwerk Blacklist Filter - Prüfung der IP-Adresse des E-Mail-Servers des Absenders gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

**NWL Filter:** Netzwerk Whitelist Filter - Autorisierung der IP-Adresse des E-Mail-Servers des Absenders gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

## O

**OS:** Operating System, den auch im deutschen Sprachraum geläufigen engl. Begriff für Betriebssystem.

## Q

**Quarantäne:** Die REDDOXX Appliance beinhaltet für alle freigeschalteten Benutzer Quarantäne-Mailboxen, welche individuell eingestellt werden können. Zusammen mit den erreichten False-Positive-Raten ermöglicht Ihnen dieses Feature die Konformität zu den geltenden Gesetzen zu erreichen.

## R

**RAID:** Ein RAID-System (Abk. Redundant Array of Inexpensive Disks, oft aber auch Redundant Array of Independent Disks) dient zur Organisation mehrerer physikalischer Festplatten eines Computers zu einem leistungsfähigen bzw. sicheren logischen Laufwerk.

**RBL Filter:** Realtime Blacklist Filter - Die sendenden E-Mail-Server werden gegen öffentliche Blacklist-Server geprüft. Für die Funktion der ausgewählten Blacklist-Server sowie die Fehlerfreiheit der Listeinträge auf den Blacklist-Servern wird keine Gewähr übernommen.

**Realm:** Der Realm ist ein Bereich, ähnlich einer Domäne, in dem man sich authentifiziert. (Siehe Kapitel: "Benutzerverwaltung - Anmeldekonfiguration")

**RVC Filter:** Recipient-Verify-Check Filter - Zum Schutz der lokalen E-Mail-Server gegen "Spamfluten" erfolgt eine Überprüfung der Empfängeradresse durch Rückfrage beim jeweiligen E-Mail-Server, ob dieser Empfänger bekannt ist. Diese Funktion ist zurzeit für Microsoft Exchange Server ab der Version 5.5 möglich.

## S

**SBL Filter:** Betreff Blacklist Filter - Abprüfung des E-Mail-Betreffs gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch

unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

**SMTP:** Simple Mail Transfer Protocol. Dieses Protokoll ermöglicht eine E-Mail mit etwas mehr auszustatten, als wenn man Sie nur einfach so versenden würde! Das Protokoll hat mehrere Funktionsmöglichkeiten. Zum einen dient es dazu, ihre E-Mails einen direkten Weg zum Empfänger finden zu lassen, zum anderen ermöglicht SMTP den Weg Ihrer E-Mail über verschiedene Server, sogenannte MTA, zu Ihrem Empfänger. Fast jeder E-Mail-Client benutzt dieses Protokoll zum Versenden der elektronischen Post.

**SRC Filter:** Sender-Receive-Check Filter- Prüft ob der Absender auch eine E-Mail entgegen nehmen würde. Eine Falscherkennung, wie z.B. bei Newslettern oder sonstigen automatisch erstellten E-Mails kann nicht ausgeschlossen werden, jedoch durch entsprechende Einträge in den Positivlisten verhindert werden.

**SWL Filter:** Betreff Whitelist Filter - Autorisierung des E-Mail-Betreffs gegen eine im Spamfinder geführte Liste. Die Einträge können sowohl benutzerbezogen als auch unternehmensweit vorgenommen werden. Die Pflege dieser Listen erfolgt manuell durch den Administrator bzw. dem Benutzer.

## T

**TCP/IP:** Transmission Control Protocol / Internet Protocol. TCP/IP ist das Protokoll, das im Internet die Verbindungen/den Datenaustausch zwischen den Computern regelt. Bei der Übertragung von Information, werden die abgeschickten Daten durch TCP in kleine Pakete zerlegt, mit einer Prüfsumme versehen (Übertragungssicherheit) und durchlaufend nummeriert (um die Zusammensetzung in der richtigen Reihenfolge zu gewährleisten). Die TCP-Pakete enthalten auch die Adressen von Absender und Empfänger (IP-Adressen).

## V

**Virenscanner:** ClamAV - Der Virenscanner untersucht die Anhänge aller E-Mails nach Viren. Gepackte Dateien werden temporär entpackt und untersucht. E-Mails, bei denen eine Virenbefall erkannt wurde, werden in einem Quarantänebereich auf dem Spamfinder gespeichert. Auf diesen Bereich hat nur der Administrator Zugriff. Ihr Spamfinder bezieht die Virensignaturen direkt vom Hersteller (ClamAV). Es wird keine Gewähr für die Aktualität der Signaturdateien sowie die Verfügbarkeit des Signaturservers übernommen. Für Schäden, die durch unerkannte Viren entstehen können, wird keine Haftung übernommen.

# 10 Index